Todo lo que no sabes sobre las nuevas amenazas
y las guerras que ya se libran en la red

Ciberguerra

Yolanda Quintana
PRÓLOGO DE MARIO TASCÓN

CATARATA

Todo lo que no sabes sobre las nuevas amenazas
y las guerras que ya se libran en la red

Ciberguerra

Yolanda Quintana
PRÓLOGO DE MARIO TASCÓN

CATARATA

Todo lo que no sabes sobre las nuevas amenazas
y las guerras que ya se libran en la red

Ciberguerra

Yolanda Quintana
PRÓLOGO DE MARIO TASCÓN

CATARATA

Índice

PRÓLOGO. EL ABC DE LA GUERRA HA CAMBIADO, AHORA ES ABCD, por Mario Tascón

INTRODUCCIÓN. DÍA Ø: COMIENZA LA CIBERGUERRA

CAPÍTULO 1. LA SORPRENDENTE HISTORIA DE AGENT.BTZ. EL ESPÍA QUE INAUGURÓ LA CIBERGUERRA

La Operación Buckshot Yankee

La visita de Bush a la NSA

Un gran catalizador

La reaparición de Agent.btz

CAPÍTULO 2. LA GUERRA EN RED: NUEVOS TERRITORIOS Y NUEVOS ACTORES

Nuevo territorio: el ciberespacio

La guerra en red

Nuevos actores: quién es quién en la ciberguerra

CAPÍTULO 3. ASÍ SE LUCHA EN LA CIBERGUERRA: DE LOS ATAQUES DDOS AL SECUESTRO DE SISTEMAS

Ataques de "Día Cero"

Software malicioso (malware)

Secuestro de sistemas: ransomware

El Internet de las Cosas y ciberguerra

Ataques a insfraestructuras críticas

Ingeniería social

Ataques DDOS

Ataques de "baja intensidad": desfiguración de webs

Nuevas tácticas: de la geometría al Big Data

Las fechas de la ciberguerra

CAPÍTULO 4. TODOS LOS SECRETOS DE LA PRIMERA ARMA CIBERNÉTICA

Una boda y la Pantalla Azul de la Muerte

Los sistemas SCADA y la reunión secreta de Obama

El virus por dentro

El hombre que descubrió que Stuxnet era un arma

Así saboteó Stuxnet la planta nuclear de Natanz

‘Un tipo de amenaza que esperamos no volver a ver nunca’

Los pacientes cero

La orden de crear Stuxnet, la primera arma cibernética

CAPÍTULO 5. LOS EJÉRCITOS DEL FUTURO

La guerra de los robots

Drones: matar a distancia

Big Data, inteligencia artificial y ‘machine learning’

CAPÍTULO 6. LA CIBERGUERRA DE LA INFORMACIÓN

Ciberespionaje: las claves del caso Snowden

Propaganda, contrainformación y censura en el ciberespacio

Las guerras del cifrado

BIBLIOGRAFÍA

NOTAS

Yolanda Quintana

Periodista especializada en Internet y movimientos sociales. Fruto de ese trabajo fue la publicación, junto a Mario Tascón, de Ciberactivismo: las nuevas revoluciones de las multitudes conectadas (Los Libros de la Catarata, 2012), un libro que anticipaba las nuevas formas de protesta y de organización política. Para eldiario.es ha cubierto el caso Snowden y otras informaciones relacionadas con las tecnologías y los derechos civiles en la red. También es ponente habitual o profesora en jornadas y cursos, y autora de diversas publicaciones e investigaciones sobre estos temas. Es secretaria general y coordinadora de la Plataforma en Defensa de la Libertad de Información (PDLI) y trabaja como responsable de comunicación, tecnologías y privacidad en una organización de consumidores.

Yolanda Quintana

Ciberguerra

DISEÑO DE CUBIERTA: Fernando Rapa Carballo

© Yolanda Quintana, 2016

© Los libros de la Catarata, 2016

Fuencarral, 70

28004 Madrid

Tel. 91 532 20 77

Fax. 91 532 43 34

www.catarata.org

Ciberguerra

isbne: 978-84-9097-175-8

ISBN: 978-84-9097-126-0

DEPÓSITO LEGAL: M-19.293-2016

IBIC: J/UR/JW

este libro ha sido editado para ser distribuido. La intención de los editores es que sea utilizado lo más ampliamente posible, que sean adquiridos originales para permitir la edición de otros nuevos y que, de reproducir partes, se haga constar el título y la autoría.

PRÓLOGO

El ABC de la guerra ha cambiado, ahora es ABCD

El siglo XX ha sido el escenario del desarrollo de diferentes tipos de armas de destrucción masiva: atómicas, biológicas y químicas —ABC (Atomic, Biological and Chemical, por sus siglas en inglés)—. Pero el siglo XXI ha venido a añadir una letra a este escalofriante abecedario: la D de "digital".

El pasado mes de abril de 2016, según un informe desvelado por el diario The New York Times, el Gobierno de Estados Unidos, a través de su Cibercomando, decidió utilizar por primera vez la guerra cibernética contra el ISIS, con el objetivo de cortar y manipular sus sistemas de comunicaciones para intentar estrangular sus sistemas de reclutamiento, de circulación de mensajes y órdenes, así como sus sistemas de pago. Hasta ahora, el Cibercomando de Estados Unidos, brazo militar de la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés), estaba concentrado en Rusia, China, Irán y Corea del Norte, los países desde los que, para los expertos norteamericanos, se estaban recibiendo la mayoría de los ataques en Internet.

Este supuso un paso más desde que, hace siete años, el secretario de Defensa del Gobierno Obama anunciara la creación de este grupo porque "sabemos que hay gobiernos que están intentando desarrollar su capacidad ofensiva en Internet. Más de un centenar de servicios de inteligencia extranjeros tratan de penetrar ilegalmente en las redes estadounidenses".

También España mostró su preocupación por este asunto y creó, aunque varios años después, en 2013, el Mando Conjunto de Ciberdefensa, un organismo similar en competencias y funciones al Cibercomando estadounidense, del que está al cargo el general de división Carlos Gómez López de Medina, un experto en telecomunicaciones.

El vector digital es, por tanto, posiblemente la mayor preocupación actual de los gobiernos que llegan tarde, aunque con recursos y medios, a este escenario.

Hace ya bastantes años, en 1996, desde el interior del Foro de Davos, el poeta y ensayista John Perry Barlow, vicepresidente de la afamada organización defensora de derechos en el ciberespacio, Electronic Frontier Foundation, advertía: “Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido que nos dejéis en paz en el pasado No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos”. Los gobiernos, por lo que vemos, tomaron rápida cuenta de la advertencia, pero para ocupar ese territorio que, como bien avisó Barlow, estaba en pleno estallido de prosperidad (e inocencia).

Las revelaciones a la prensa mundial del consultor tecnológico estadounidense y antiguo miembro de la NSA, Edward Snowden, además de conseguir acabar con la inocencia digital de una parte del público occidental, incluso, me atrevo a decir, de muchos gobiernos de nuestro entorno, pusieron de manifiesto la voracidad de control digital de las fuerzas de seguridad, favorecidas por la seguridad en el eje seguridad-libertad. El programa PRISM, que sacó a la luz las filtraciones de Snowden, era una aplicación de técnicas avanzadas de Big Data para analizar millones de comunicaciones de ciudadanos occidentales, incluso de sus gobiernos, aliados de quien los espiaba.

Los ataques terroristas de Nueva York, Boston, Londres, París, Madrid, Bruselas, directos al corazón de Occidente, forman parte de una nueva forma de guerra donde, como mínimo, la comunicación a través de Internet tiene un peso importante. Entre los sistemas que ahora protegen los gobiernos no están solo las instalaciones eléctricas o de comunicaciones, las estaciones de tren y las centrales nucleares, sino que ahora se suman las redes de comunicaciones y, a medida que los avances con el Internet de las Cosas convierten nuestras ciudades y casas en entornos más cómodos y funcionales, también los hacen más atractivos para lanzar a través de ellos ataques o bloqueos, por lo que son objeto de interés tanto para defensores como para atacantes.

Los gobiernos suspiran no solo por controlar las comunicaciones del enemigo, sino incluso por poder realizar intrusiones en sus sistemas

digitales sabiendo que eso es como atacar el sistema nervioso central de un ser humano. Un disparo directo al hipotálamo sin necesidad de descuartizar manos y piernas; esa es la metáfora aplicada al enemigo con la que sueñan los ejércitos cibernéticos. Se trata de una guerra en la que, por fuerte que sea el contrario, si conseguimos afectar a su médula espinal, la fuerza no servirá de nada.

Y podemos ir más allá, en un tirabuzón y doble salto mortal, cuando, además de lo que sería un "aséptico" asalto a los centros de datos de un país o la toma de control de una central eléctrica, nos enfrentemos también a la amenaza de que puedan controlarse los algoritmos, la inteligencia artificial y, por extensión, los robots militares autónomos.

No nos referimos solo a los drones y vehículos semiautomáticos, y no es ciencia-ficción. En 2015, más de un millar de científicos, entre los que se encuentran el físico Stephen Hawking, Steve Wozniak, uno de los fundadores de Apple, y Elon Musk, el dueño de Tesla Motors, firmaron un manifiesto contra robots militares autónomos que puedan funcionar sin que seres humanos los manejen. Las ventajas que tienen esas nuevas armas dotadas de inteligencia artificial las convierten en un nuevo y deseado objeto, por lo que, advierten los firmantes, "solo es cuestión de tiempo" que esta tecnología se venda en el "mercado negro y pase a manos de terroristas, dictadores y señores de la guerra". Y si no consiguen controlar los robots inteligentes, todos los terroristas y gobiernos sueñan con lograr asestar, en el país o en las filas enemigas, un imponente golpe: un ataque de día cero. ¿Qué es el ataque de día cero? La autora del libro, Yolanda Quintana, lo explica mucho mejor de lo que pueda hacerlo yo en las siguientes páginas.

Quizás esa nueva D que eleva este nuevo tipo de armas a la categoría de destrucción masiva no sea la D de "digital" y sea la D de "día cero".

Mario Tascón

Introducción

Día Ø: comienza la ciberguerra

Estamos en guerra. Y me pareció que lo más honesto era contarle en qué consiste.

La guerra en red, Manuel Castells

El término “ciberguerra” no es nuevo. Fue acuñado por el Centro de Estudios de Defensa norteamericano Rand Corporation a principios de los años noventa del siglo pasado para referirse a un tipo de conflicto no conocido hasta entonces en el que las tecnologías de la comunicación serían la principal arma —a la vez que campo de batalla— y en el que las estructuras en red —como grupos terroristas o de delincuencia organizada distribuidos— iban a contar con ventaja.

Desde entonces, las tecnologías —sistemas, dispositivos y herramientas— han multiplicado su presencia y su capacidad de intervención —son cada vez más rápidas, ubicuas y sencillas— y han aparecido nuevas amenazas, como el terrorismo integrista islámico, que se adaptan a estas nuevas formas de conflicto más fácilmente que sus oponentes.

La propaganda en redes sociales para el reclutamiento y adoctrinamiento, nuevos ejércitos que en lugar de por soldados están integrados por “robots” y ataques cibernéticos como el borrado o manipulación de datos o el secuestro de sistemas (ransomware) que pueden comprometer instalaciones estratégicas, son algunas caras de este nuevo fenómeno en el que conviven actores tradicionales (los Estados con sus conflictos bilaterales o las empresas con sus guerras comerciales) y otros que en los últimos años han emergido poniendo en riesgo la seguridad mundial.

Junto a ello, nuevas realidades tecnológicas como el Internet de las Cosas aumenta las capacidades de la guerra y los sistemas de defensa, a la vez que crece el riesgo de captura de piezas a favor del

enemigo si este las hackea. Cambia el concepto de “asalto de una posición” de las guerras tradicionales: ahora se pueden hackear drones o sensores para distorsionar la sensibilidad enemiga o su capacidad de ataque o aprovechar las capacidades de cálculo del enemigo sin que este lo sepa.

Por otro lado, el aspecto económico de la ciberguerra no es baladí. Hay nuevos sistemas de pago de armas mediante bitcoins y la web oculta o web profunda es escenario habitual de estas transacciones.

Frente a ello, es razonable la preocupación sobre si los Estados y las empresas de sectores sensibles (comunicaciones, energéticas, financieras…) están convenientemente preparados y sobre cuál es el precio, en derechos y libertades, que los ciudadanos vamos a pagar en aras de una seguridad que tal vez no sea posible.

En los últimos años hemos visto noticias sobre una central nuclear saboteada por un virus, apagones de luz provocados por ataques informáticos o misiles Patriot dirigidos a distancia por alguien desconocido sin autorización para ello. Estos incidentes reflejan, por si alguien lo dudaba, que las guerras del futuro ya han empezado. Son conflictos donde la infantería ha dado paso a las máquinas, los ataques se ejecutan con líneas de código de programación y el terreno a ganar ya no es físico, sino virtual.

Pero ¿en qué consisten y cómo se desarrollan? ¿Cuál es el alcance real de las nuevas amenazas? ¿Qué papel tiene en todo ello la tecnología y por qué es distinto de los conflictos armados del pasado? ¿Están nuestras leyes preparadas? ¿Qué problemas éticos se abren? ¿Cuál es el impacto en nuestros derechos y libertades?

Este libro pretende explicar, de forma sencilla, todas estas cuestiones y ofrecer las claves de las principales novedades que presenta este nuevo escenario, sorprendente en muchos aspectos. También desmonta mitos y contextualiza episodios que hasta ahora no se habían explicado suficientemente, como el papel de los Estados en gran parte de los ciberataques que se producen. Por último, abre una reflexión sobre los debates, legales y éticos, que plantean estos nuevos conflictos y que, como sociedad, tenemos que resolver.

Capítulo 1

La sorprendente historia de Agent.btz, el espía que inauguró la ciberguerra

La primera víctima de una guerra es la verdad.

Senador Hiram W. Johnson, 1917

La actual ciberguerra quedó oficialmente inaugurada tras la entrada en acción de Agent.btz, un espía que fue capaz de causar lo que se dio a conocer como "la peor violación de los equipos militares estadounidenses de la historia". El incidente tuvo tanto impacto que años después se sigue recordando así en libros especializados y en documentos estratégicos del Ejército.

Se cuenta que todo habría empezado cuando alguien dejó tirada una unidad flash USB en el aparcamiento de una instalación de una base militar norteamericana en Oriente Medio en algún momento de 2008. La técnica se conoce como candy drop ("tirar un caramelo") y se usa para saltarse una protección básica frente a las intrusiones informáticas: los ordenadores de sistemas críticos, como los de los ejércitos, utilizan un mecanismo de seguridad que se conoce como "muro de aire" (air gap o air wall), que no es otra cosa que su aislamiento físico de cualquier tipo de red, tanto local como Internet. Con esta precaución se pretende evitar que los equipos sean alcanzados por software malicioso que dé lugar a incidencias que pueden ser de enorme gravedad, como el "secuestro" del sistema o el acceso a la información que contiene.

Sin embargo, Agent.btz, a quien podemos considerar el primer espía de la ciberguerra moderna, sabía cómo superar esa barrera.

Conviene aclarar que este "agente" es un programa de software. Agent.btz, igual que ocurre en las películas de espías de carne y hueso, ha tenido varias identidades que se le fueron asignando según fue siendo descubierto. Así, se le conoce también como Autorun o, en menor medida, Trojan.Minit. También, como muchos

agentes “clásicos”, supo transformarse y, años después, volvería salir a la luz con otras denominaciones.

En 2008, Estados Unidos contaba, según las cifras que el Ejército hizo públicas entonces, con 716 instalaciones militares fuera del país, aunque aquella documentación omitía datos sobre lugares con operaciones abiertas como Irak o Afganistán (Departamento de Defensa, 2009). Para hacernos una idea del despliegue, en esa fecha estaban destinados en aquellos lugares más de 140.000 soldados en el primer caso y 33.000 en el segundo[1]. Todo ello sin contar los civiles o contratistas extranjeros vinculados al ejército.

En el aparcamiento de una de esas instalaciones habría aparecido un día una memoria extraíble del tamaño de un cigarrillo electrónico. El experto en robots militares y asesor de Obama para asuntos de Defensa en su primera campaña presidencial, P. W. Singer, se refiere al episodio con esta metáfora en un libro reciente:

En 2008, un soldado estadounidense caminaba por un estacionamiento de una base militar estadounidense de Medio Oriente cuando reparó en una chocolatina sin envolver tirada en el suelo. Sin saber quién la había dejado o cuánto tiempo llevaba allí, decidió llevar la chocolatina a la base y comérsela para el almuerzo. Suena absurdo e incluso un poco desagradable, ¿verdad? Bueno, sustituyan un ‘pen drive’ por esa barra de chocolate y tendrán la historia de cómo comenzó Buckshot Yankee, una de las mayores violaciones cibernéticas en la historia militar de Estados Unidos (Singer y Friedman, 2014).

En aquella memoria que se habría instalado en un puerto USB de un ordenador portátil conectado con el Mando Central de Estados Unidos estaba Agent.btz.

El espía “se extendió por sistemas clasificados y no clasificados sin ser detectado. Este software estableció el equivalente digital a una cabeza de puente, desde donde se transfirieron miles de archivos de datos a servidores bajo control extranjero”, contaba hace unos años

un boletín del Instituto de Estudios Estratégicos del Ejército español (Caro Bejarano, 2013).

Cuando Agent.btz fue identificado, se supo que era una variante de lo que en argot informático se denomina “gusano”, un programa malicioso que, a diferencia de los virus, tiene la propiedad de duplicarse a sí mismo. En concreto, del gusano llamado SillyFDC, descubierto en enero de 2007[2], aunque existían versiones previas de 2005 e incluso anteriores.

Agent.btz tendría capacidad “para examinar datos de los equipos, puertas traseras abiertas, y enviar, a través de esas puertas, documentos e información clasificada”, según informaría más tarde el Ejército norteamericano.

La Operación Buckshot Yankee

La primera señal de problemas llegó en octubre de 2008. OPS1 es un edificio cuadrado de baja altura que no llama la atención en el campus de 660 acres de la NSA. En una habitación sin ventanas trabaja un grupo de elite formado por ingenieros, matemáticos y físicos que rastrea la red informática del Ejército en busca de problemas. Se trata del equipo de Operaciones de Redes Avanzadas de la NSA, constituido dos años atrás.

Uno de estos jóvenes analistas descubre “una señal misteriosa que emana de las profundidades de la red de ordenadores clasificada de los militares de Estados Unidos. Al igual que un espía humano, una pieza de software encubierta en el sistema supuestamente seguro estaba tratando de enviar mensajes codificados de nuevo a su creador”, según contaría años después The Washington Post al reconstruir el incidente a partir de fuentes del Ejército (Nakashima, 2011).

Había comenzado la Operación Buckshot Yankee. El Pentágono iba a tardar casi 14 meses en limpiar Agent.btz de sus redes militares.

Los analistas de la NSA (“los mejores guerreros cibernéticos del Gobierno”, según los describió el periódico norteamericano de referencia) habían descubierto a Agent.btz en su “Internet secreto” o SIPRNet (Secret Internet Protocol Router Network), un entorno absolutamente seguro que los departamentos de Defensa y de Estado utilizan para transmitir material clasificado, pero no información sensible. El SIPRNet o NIPRNet (Weinberger, 2010), la versión secreta de Internet que opera el Departamento de Defensa de Estados Unidos, no era conocido hasta las filtraciones por parte de WikiLeaks de los cables diplomáticos que procedían de este canal, y sus siglas quedaban reflejadas en los documentos publicados. Se trata de un sistema de redes de ordenadores interconectados que excede las prestaciones del protocolo básico TCP/IP que usamos normalmente. Según datos del Pentágono,

puede contar con entre 400.000 y 500.000 usuarios.

Agent.btz también había infectado el sistema de comunicación del Mando Conjunto de Inteligencia Global, que lleva la información de alto secreto a los funcionarios de Estados Unidos en todo el mundo, una red clasificada, separada del Internet público, que albergaba algunos de los secretos más importantes de los militares, incluyendo los planes de batalla utilizados por los comandantes en Afganistán e Irak.

Los informáticos de la NSA no podían determinar en ese momento quién había creado el programa o por qué, a pesar de que llegarían a sospechar del servicio de inteligencia ruso; así se iba a dar a entender en las sucesivas informaciones sobre el incidente.

Tampoco podían determinar cuánto tiempo había estado allí Agent.btz, pero pronto se dedujeron los medios sorprendentemente sencillos de transmisión que tenía: Agent.btz se transportaba inadvertidamente en una unidad USB cotidiana, lo que le permitió entrar en el sistema secreto y "comenzar a buscar los documentos que debía robar", según contaría el Ejército. Luego se extendió propagando copias de sí mismo en otras memorias USB.

Los agentes de Operaciones de Redes Avanzadas de la NSA determinaron que la infracción era grave después de días intensos de investigación.

Agent.btz es un archivo DLL[3]. El modo de replicarse era el siguiente: cuando una unidad de memoria (memoria USB) o cualquier otro disco duro externo estaba conectado a un ordenador infectado con Agent.btz, este detectaba la unidad, dejaba su copia en él y un archivo autorun.inf con instrucciones para ser ejecutado. Cuando un equipo limpio reconocía una unidad extraíble recién conectada, sería, por defecto, detectado el archivo autorun.inf en él. A continuación, lo abriría y seguiría sus instrucciones para cargar el software malicioso.

Otra forma de infección consistió en que, cuando desde un equipo limpio se exploraba una unidad compartida (una impresora en red, por ejemplo) que tenía a Agent.btz en ella y el archivo autorun.inf correspondiente, se ponía en marcha el mismo proceso (el archivo

sería abierto automáticamente y seguiría sus instrucciones para cargar el software malicioso. Una vez infectado, haría lo mismo con otras unidades extraíbles conectadas a él u otros equipos de la red).

La visita de Bush a la NSA

Mientras esto ocurre en el mundo virtual, en el real el presidente saliente George Bush está realizando una de las visitas que marcan la habitual ronda de despedidas de un mandato. En ese momento ya se da por prácticamente segura la victoria de Obama sobre el candidato republicano, McCain, en las elecciones que tendrán lugar en menos de dos semanas. En el último mes, las encuestas han confirmado el despegue de Obama y las de esos días muestran una diferencia de hasta 13 puntos a favor del gobernador de Illinois[4].

El 24 de octubre, Bush se ha desplazado a la sede de la todopoderosa NSA, a 33 kilómetros al noreste de Washington D. C. El complejo es conocido como "El fuerte", debido a su ubicación en Fort Meade, Maryland, y a las extraordinarias medidas de seguridad que tienen sus instalaciones. El recinto tiene su propia salida a la carretera Baltimore-Washington, señalizada como "solo para empleados de la NSA".

La agencia, durante muchos años desconocida para el gran público, saltaría a primera línea de la actualidad años más tarde, al conocerse sus prácticas de espionaje masivo gracias a los documentos desvelados por Edward Snowden. Entre otras operaciones secretas, se pudo ver cómo en sus talleres se alteraban de manera clandestina equipos informáticos para introducirles dispositivos o programas de rastreo.

A las 12.30, Bush hace una declaración institucional, de protocolo, ante los medios que se han desplazado para cubrir la visita. Le acompañan el vicepresidente, Dick Cheney; el teniente general Keith Alexander, director de la NSA, y el director de Inteligencia Nacional, Mike McConnell:

Quiero agradecer su hospitalidad al general Alexander, al

vicepresidente y al director McConnell. Hemos estado aquí, en la NSA, en primera línea de la protección del pueblo estadounidense. En cada visita, quedo impresionado por el calibre de las personas que trabajan aquí, la cantidad de energía que invierten en su trabajo y su profundo deseo de encontrar al enemigo y llevarle ante la justicia antes de que nos vuelvan a hacer daño.

Desde el 11S, las personas de este edificio han hecho lo que el país espera que hagan: trabajar tan duro como sea necesario para ayudar a proteger a los Estados Unidos de América. El trabajo de la NSA es absolutamente vital, y me gustaría que todos los ciudadanos pudieran cumplir con la gente que trabaja aquí y darse cuenta de lo inteligentes que son, lo capaces que son, y el entusiasmo con el que están cumpliendo su deber.

Por lo tanto, general, gracias por su hospitalidad. Hemos disfrutado de la visita y apreciamos el esfuerzo que está llevando a cabo para proteger el territorio nacional[5].

Como vemos, su discurso no hace ninguna referencia al incidente que se está gestionando a solo unos metros de donde se encuentra. Sin embargo, ese preciso día, cuando el responsable de la protección de los sistemas informáticos de la NSA, Richard C. Schaeffer Jr., se encontraba participando en la reunión informativa con el presidente, un ayudante le habría entregado una nota advirtiéndole de la violación.

A las 16.30, Schaeffer entró en la oficina del general Keith Alexander, director de la NSA. “Tenemos un problema”, dijo.

Esa misma noche, los funcionarios de la NSA informaron a los niveles más altos del Gobierno de Estados Unidos (el jefe del Estado Mayor Conjunto de Estados Unidos, el subsecretario de Defensa y altos líderes del Congreso) sobre el incidente causado por Agent.btz. Y los agentes de Operaciones trabajaron durante toda la noche para

encontrar una posible solución. Después de varias pruebas, la derrota de la amenaza pasó por neutralizar Agent.btz de cualquier parte de las redes gubernamentales en las que se había extendido, un largo proceso que implicó el aislamiento de equipos individuales desconectándolos de la red, su limpieza y el formateo de discos duros.

Un actor clave en esta tarea habría sido la denominada Oficina de Operaciones de Acceso a Medida (TAO) de la NSA, los hackers (o crackers[6], según se mire) del espionaje norteamericano. Son la unidad militar de ofensiva cibernética. La TAO es una unidad activa desde los años noventa. Sus agentes, entre otras actividades, identifican, monitorizan y se infiltran en los sistemas informáticos utilizados por entidades extranjeras.

Estos especialistas "exploraron" fuera de las redes de los militares para buscar Agent.btz e identificaron nuevas variantes del malware, "ayudando a los defensores de la red a neutralizarlos antes de que infectaran las computadoras militares", según contaron años después.

Cuando la TAO entró en acción en el caso de Agent.btz en la NSA, se debatió "si usar herramientas ofensivas para neutralizar el malware en redes no militares, incluyendo las de otros países". Una tensión que siempre va a estar presente en la "ciberguerra": la línea que separa el ataque de la defensa y el riesgo de militarización de ámbitos civiles, como las infraestructuras críticas (suministro eléctrico, comunicaciones, etc.). Aparentemente, en aquel momento se rechazó esa opción porque "Agent.btz parecía ser un acto de espionaje, no un ataque directo, y no justificaba una respuesta tan agresiva".

Al tiempo que se trabajaba en neutralizar Agent.btz de los ordenadores del Gobierno, se elevó el nivel de amenaza a la seguridad de los militares. Unas semanas más tarde, en noviembre, se emitió una orden de prohibición del uso de memorias USB en cualquier equipo del Departamento de Defensa en todo el mundo. Agent.btz se había extendido ampliamente entre los equipos militares en todo el mundo, especialmente en Irak y Afganistán. La prohibición generó la reacción de los agentes en el terreno, que dependían de las unidades para descargar las imágenes de combate

o compartir informes posteriores a la acción.

Esta orden fue, precisamente, la primera noticia que apareció en un medio de comunicación sobre el incidente del que entonces nada se sabía y que ha sido reconstruido a partir de versiones muy posteriores. La exclusiva fue lanzada por el blog de seguridad de la revista Wired, "Danger Room", el 19 noviembre de 2008. Obama ya era presidente electo.

El mandato de prohibición fue firmado por el comandante del Mando Estratégico de Estados Unidos, según un correo electrónico interno del Ejército. Se aplicaba tanto a las redes secretas SIPR como a las no clasificadas NIPR. La suspensión, que incluía todo, desde discos duros externos a "disquetes", debía aplicarse "inmediatamente".

"Se cree que el cese del uso de todos los medios de almacenamiento USB estará en vigor hasta que los dispositivos estén correctamente escaneados y se compruebe que están libres de malware", explicaba uno de los correos electrónicos que transmitían la orden a las unidades. "Con el tiempo, podrá permitirse el uso de algunos dispositivos aprobados por el Gobierno en ciertas 'misiones críticas', pero no clasificadas, y según las circunstancias. Dispositivos de propiedad personal, o no autorizados, están prohibidos de aquí en adelante", se decía.

Además, se advertía: "Para asegurarse de que las tropas militares y civiles están observando la suspensión, los equipos de seguridad del Gobierno están llevando a cabo exploraciones diarias y ejecutando scripts personalizados en NIPRNet y SIPRNet para asegurarse que no se ha introducido malware". "Cualquier descubrimiento de malware dará lugar a la apertura de un informe de incidente de seguridad y será referido al oficial de seguridad para la acción oportuna", concluían.

Unos días después, el 28 de noviembre, Los Angeles Times amplía la información, revelando que, a causa de su gravedad, se había comunicado a Bush (entonces ya presidente en funciones) la existencia "del ataque": "Altos mandos militares tomaron la medida excepcional de informar al presidente Bush esta semana sobre un ataque electrónico grave y generalizado en los ordenadores del

Departamento de Defensa que puede tener su origen en Rusia".

La NSA y los militares investigaron durante meses cómo se produjo la infección. Se recuperaron miles de unidades de memoria flash, muchas de las cuales estaban infectadas. La tasa de nuevas infecciones remitió finalmente a principios de 2009 y la prohibición de las memorias USB se levantó de forma parcial meses después.

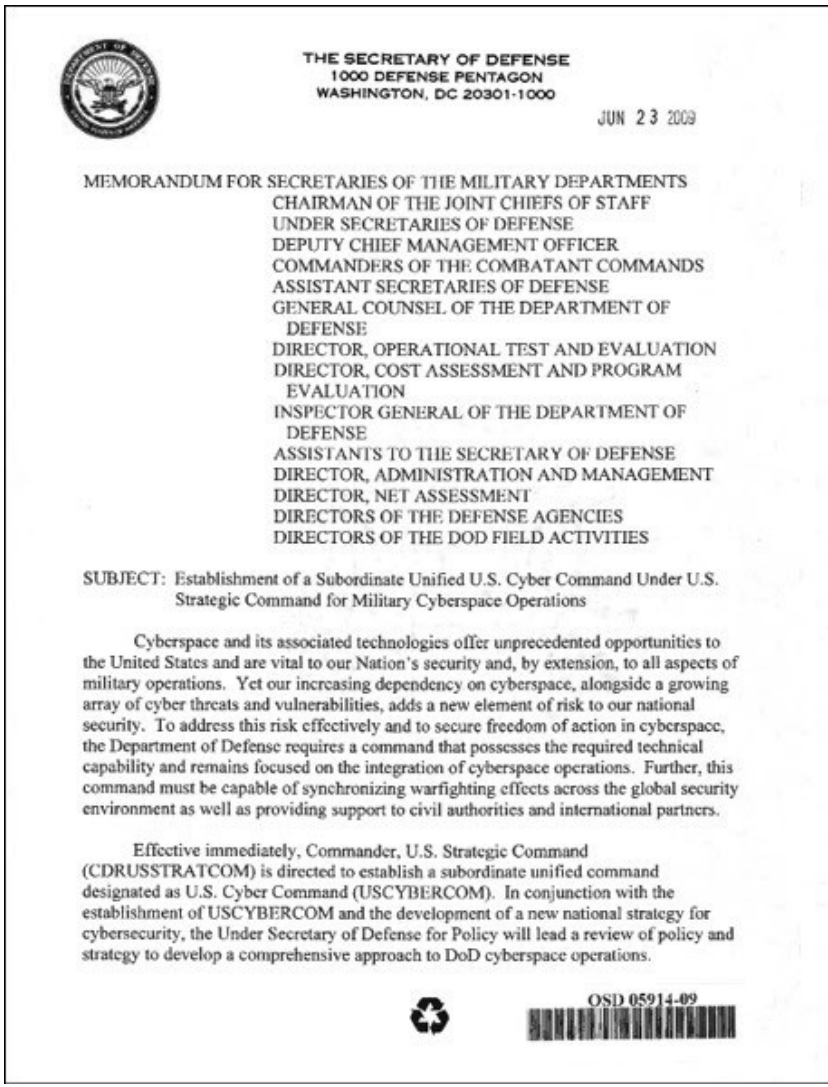
El 23 de junio de 2009 se produce la primera consecuencia de alcance del caso Agent.btz: el secretario de Defensa, Robert Gates, ordena la creación de un nuevo Mando Cibernético de Estados Unidos.

Hasta ahora existía un Cibermando provisional vinculado a las Fuerzas Aéreas con el teniente general William T. Lord al frente. El proceso para la creación del mismo se inició en 2005, cuando la Fuerza Aérea modificó la declaración de su misión al ampliar al ciberespacio sus dominios tradicionales: el aire y el espacio (Brenner, 2013). Entró en funcionamiento en 2007, pero la fecha de su constitución se fue demorando hasta octubre de 2008. En esa fecha, coincidiendo con el caso de Agent.btz, en lugar de eso, la Fuerza Aérea puso el proyecto en espera con el fin de "hacer una nueva evaluación" sobre la manera correcta de abordar el establecimiento de un Mando Cibernético.

En julio de 2009, el organismo queda en suspenso y el general Bill Lord pierde sus competencias. La revista Air Force Magazine publica un artículo sobre este final: "On pause, but not abandoning".

Con la orden del secretario de Defensa, Robert Gates, una cosa estaba bastante clara: la NSA estaría al frente de este comando emergente. Gates recomendaba que el director de la NSA, el teniente general Keith Alexander, también se convirtiese en el jefe de la nueva fuerza de la red, consiguiendo así su cuarta estrella, y sugería que el comando estableciera su sede en Fort Meade, Maryland, donde se ubica la NSA.

Figura 1



THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUN 23 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations

Cyberspace and its associated technologies offer unprecedented opportunities to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.

Effective immediately, Commander, U.S. Strategic Command (CDRUSSTRATCOM) is directed to establish a subordinate unified command designated as U.S. Cyber Command (USCYBERCOM). In conjunction with the establishment of USCYBERCOM and the development of a new national strategy for cybersecurity, the Under Secretary of Defense for Policy will lead a review of policy and strategy to develop a comprehensive approach to DoD cyberspace operations.

OSD 05914-09

Fuente: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf

El Cibermando debería estar operativo en octubre de 2010. Justo un mes antes, sale a la luz lo que sería la primera versión detallada del

incidente de Agent.btz. Se trata de un artículo que el subsecretario de Defensa norteamericano, William J. Lynn III (2010), escribe en el número de septiembre de Foreing Affairs confirmando oficialmente lo que denominó “la peor intrusión que hayan sufrido nunca los ordenadores militares”.

En su artículo, Lynn narra los pormenores del ataque y se refiere por primera vez al USB abandonado en un aparcamiento y “puesto allí por una agencia de inteligencia extranjera”. Distintos medios, como The New York Times, se hacen eco de la publicación de estas revelaciones (Knowlton, 2010). La versión de Lynn es la historia oficial del caso Agent.btz y, como tal, se sigue contando.

Un gran catalizador

Sin embargo, años más tarde las autoridades reconocieron que no había pruebas de cómo surgió Agent.btz ni si tuvo éxito en la comunicación con un ordenador principal o en poner documentos secretos en poder del enemigo (Shachtman, 2010).

Gran parte de la energía se dedicó a tratar de encontrar el "paciente cero". "Resultó ser demasiado complicado", admitieron después. "Nunca pudimos determinar: 'Esa es la unidad de disco USB'", declararon los militares a The Washington Post (Nakashima, 2011).

Nunca se informó si Agent.btz había llegado a "robar" algún tipo de información o documento ni cuál o cuáles habrían sido. Tampoco si había sido creado para esta misión específica. Su funcionamiento (entrar en un sistema y ponerse "en contacto" con su fuente original) no difiere a lo que cualquier botnet malware (virus que convierte el ordenador en un robot) hace una vez que ha infectado un sistema, como advertía la experta en seguridad informática de Wired, Kim Zetter (2011d).

Tampoco el origen de la infección, por más que haya prosperado en la memoria colectiva la historia del pen drive, parece —como es lógico, por otra parte— claro. El propio The Washington Post, en su historia de 2011, reproduce declaraciones de fuentes militares que admiten que un escenario más probable habría sido que un soldado americano, funcionario o contratista en Afganistán —donde se produjeron el mayor número de infecciones— fueran a un cibercafé, utilizan una unidad de disco USB en un ordenador infectado y luego lo insertan en la unidad de una máquina clasificada.

"Sabíamos con bastante seguridad que el mecanismo había sido alguien que hace algo que no debería hacer en contraposición a alguien que había sido capaz de entrar en la red", declaró al Post un exfuncionario. La revista Wired se refirió al incidente como "leyenda urbana" (Poulse, 2010).

Sin embargo, a pesar de las inconsistencias, el caso de Agent.btz, tal como fue reconstruyéndose posteriormente, con filtraciones muy medidas, un eslogan inmejorable (“el peor ataque a las redes informáticas militares de Estados Unidos”) y una buena historia bien contada (“todo comenzó con una memoria UBS tirada en el aparcamiento de una base militar”, dice la entrada de la Wikipedia del incidente que aún puede leerse hoy) iba a tener grandes consecuencias.

Fue nada menos que el origen del primer Mando Cibernético militar del mundo y, algo nada trivial, que recayese sobre el director de los servicios de inteligencia, Keith Alexander, al frente de la NSA desde 2005.

Aunque en 2008, cuando ocurre este episodio, no es conocido, Alexander saltará a las portadas de todo el mundo años después, en junio de 2013, por ser el responsable de la NSA cuando sale a la luz el caso Snowden y el inspirador de la estrategia de espionaje “atrápalotodo” denunciada por el joven exanalista.

Se le atribuye la frase: “En lugar de buscar una aguja en un pajar, recojamos el pajar completo”, en referencia a la capacidad de la agencia de recopilar todo tipo de información de las comunicaciones electrónicas de cualquier persona.

En marzo de 2014, Alexander dejará la NSA a consecuencia de las filtraciones de Snowden. Ya fuera del Ejército montará una consultora sobre seguridad informática que ofrece sus servicios a bancos y otras empresas sensibles por un millón de dólares al mes (Dougherty y Hamilton, 2014).

“Él es el único hombre en la Tierra capaz de crear un problema en virtud de su control de la Inteligencia y luego ofrecer una solución en virtud de su condición de militar”, dijo de él un exoficial.

La Operación Buckshot Yankee reforzó el argumento a favor de la creación de un Comando Cibernético y, según The Washington Post, le dio a Alexander la palanca para presionar en el caso y defender ante los demás que el nuevo comando debía utilizar las capacidades de la NSA para obtener inteligencia extranjera con el objeto de defender los sistemas de los militares. “Fue un gran catalizador”,

confesó el propio Alexander al Post.

La nueva organización iba a contar con una plantilla de 750 personas y un presupuesto de 155 millones de dólares. Comenzó a operar el 31 de octubre de 2010, con Alexander a la cabeza. Su emblema contiene un anillo interior dorado con una extraña secuencia de números y letras: “9ec4c12949a 4f31474f299058ce2b22a”. Resultó ser un resumen de la misión que iba a llevar a cabo después de pasarle por un algoritmo de cifrado:

USCYBERCOM planea, coordina, integra, sincroniza y lleva a cabo actividades de dirección de las operaciones y defensa de las redes específicas de información del Departamento de Defensa; y se prepara para, cuando así se le indique, llevar a cabo operaciones militares de amplio espectro en el ciberespacio a fin de garantizar las acciones en todos los dominios [tierra/mar/aire/espacio], y la libertad de acción de Estados Unidos y sus aliados en el ciberespacio y negar lo mismo a nuestros adversarios.

Recién llegado a la presidencia, Obama impulsará las acciones que la Administración Bush había iniciado en este terreno, lo que no se llegaría a saber hasta años después. Entre ellas, la Operación Juegos Olímpicos, que supondrá el desarrollo de la primera arma cibernética, con enormes consecuencias.

Arrancaba, oficialmente, la ciberguerra. Misión cumplida.

La reaparición de Agent.btz

Años después, aparecerían nuevos virus cuyos códigos presentan similitudes con Agent.btz (Gostev, 2014). Agent.btz era un gusano informático autorreplicante, no solo un troyano y un malware con docenas de diferentes variantes. Las variantes iniciales del gusano se crearon en 2007 y ya para 2011 se habían detectado un gran número de sus modificaciones.

Los militares estadounidenses no fueron las únicas víctimas del gusano. En pocos años, Agent.btz se extendió por todo el mundo con una dinámica llamativa: durante tres años (2011-2013), el número de infecciones causadas por Agent.btz disminuyó de manera constante. Sin embargo, los diez principales países afectados cambiaban muy poco, con Rusia como líder en términos de la cantidad de infecciones (24.111 en 2011), seguido de España (9.423), Italia (5.560) y Kazajstán (4.412).

La empresa de seguridad rusa Kaspersky encontró “restos” de Agent.btz en otros virus protagonistas de futuras operaciones de espionaje como Octubre Rojo, Turla, Flame y Gauss. Según Kaspersky:

Es posible considerar Agent.btz como un cierto punto de partida en la cadena de creación de varios proyectos diferentes de ciberespionaje. La historia bien publicitada de cómo se infectaron las redes militares de Estados Unidos podría haber servido como modelo para nuevos programas de espionaje que tienen objetivos similares, mientras que sus tecnologías fueron claramente estudiadas en gran detalle por todas las partes interesadas. ¿Son las mismas personas detrás de todos estos programas? Es posible, pero los hechos no pueden probarlo.

Así se construyó el caso Agent.btz

2007 Febrero. Surgen las primeras variantes de Agent.btz: Se identifica el gusano SillyFDC, que se propaga copiándose a sí mismo a las unidades extraíbles[7].

2008 26 de junio. La empresa F-Scure identifica una amenaza a la que bautiza como "Agent.btz". Se asigna ese nombre porque es el siguiente de la secuencia usada en la empresa: agent.bty. Se trata de un gusano que se extiende creando un archivo autorun.inf en la raíz de cada unidad con un archivo .DELL malicioso[8].

Octubre. Posible fecha de infección de los equipos del Ejército norteamericano.

24 de octubre. Bush visita la NSA. Durante su reunión con los mandos operativos, un ayudante entrega una nota a uno de ellos (Schaeffer) advirtiéndole de la violación, según la versión del Post de años después. A las 4.30 pm, Schaeffer entró en la oficina del general Keith Alexander, director de la NSA, y le dijo: "Tenemos un problema".

4 de noviembre. Obama es elegido presidente de Estados Unidos. En los siguientes días tendrá varias reuniones con Bush para preparar el traspaso de poderes. El mandatario saliente le recomienda seguir con dos campañas en marcha: el uso de drones en Pakistán y la operación en clave denominada "Juegos Olímpicos", que no saldrá a la luz hasta cuatro años después (véase el capítulo 4).

19 de noviembre. El blog Danger Room de la revista Wired ofrece en exclusiva la primera información sobre el incidente tras conocer la prohibición de usar pen drives en equipos militares al acceder a uno de los correos en los que se transmite la orden (Shachtman, 2008).

28 de noviembre. El diario Los Angeles Times informa del

ataque: “Pentagon computer networks attacked” (Barnes, 2008).

30 de noviembre. Se publican los primeros detalles técnicos sobre el “gusano”, su forma de propagación y su funcionamiento en un blog especializado sobre seguridad informática[9].

2009 20 de enero. Obama toma posesión como 44º presidente de Estados Unidos. En los primeros meses de su mandato ordenará en secreto acelerar las operaciones de ataques informáticos, entre ellas Juegos Olímpicos.

23 de junio. Orden de creación del Mando Cibernético[10]. La NSA estaría al frente y se recomendaba que el director de la NSA, el teniente general Keith Alexander, también se convirtiese en el jefe de la nueva fuerza de la red.

2010 Abril. Comparecencia de Keith Alexander ante el comité del Senado que estudia su nombramiento[11].

Julio. Estalla otra crisis, sin aparente relación: el caso Stuxnet.

25 de agosto. Primera confirmación oficial del incidente causado por Agent.btz. El subsecretario de Defensa norteamericano, William J. Lynn III (2010), publica un artículo en el número de septiembre de Foreing Affairs con detalles no conocidos del caso, como su origen en una memoria USB abandonada intencionadamente “por una agencia de inteligencia extranjera” en el aparcamiento de una base militar en Oriente Medio.

Noviembre. El Mando Cibernético está completamente operativo (Ackerman, 2010).

2011 Diciembre. Tres años después de la infección masiva, un amplio artículo en The Washington Post ofrece detalles hasta entonces no desvelados a partir de fuentes del Ejército. A pesar de que, por primera vez, se pone en duda la versión del pen drive abandonado en el aparcamiento, no se aclaran cuestiones clave, como si realmente se trató o no de un ciberataque

dirigido o si hubo algún tipo de daño.

Capítulo 2

La guerra en red: nuevos territorios y nuevos actores

El ciberespacio, en tanto que dominio global dentro del entorno de la información, es uno de los cinco dominios interdependientes, los otros son los dominios físicos son aire, tierra, mar y espacio.

Estado Mayor Conjunto de los Estados Unidos (2013)

Cuando la gente me pregunta dónde vivo, la respuesta más honesta es en Internet[12].

Edward Snowden

Nunca se sabe el alcance de un ataque. A las 13.07 horas del martes 23 de abril de 2013, la cuenta de Twitter de la principal agencia de noticias del mundo, Associated Press (AP), con dos millones de seguidores, emitía la siguiente alerta: "Última hora: dos explosiones en la Casa Blanca. Obama está herido".

Un minuto después, a las 13.08 horas, el índice de la bolsa de Wall Street comenzó una caída en picado, descendiendo 150 puntos. A las 13.13 h., cuando desde otras cuentas se desmintió la información, el Dow Jones recuperó nuevamente su nivel anterior. Sin embargo, durante esos tres minutos, el falso tuit había "borrado" del mercado 136.000 millones de dólares, según Bloomberg.

Justo 55 minutos antes de aquello, a las 12.12 horas, algunos miembros de la redacción de AP habían recibido el siguiente correo electrónico[13]:

Enviado: Tue 4/23/2013 12:12 PM

De: [nombre de un funcionario de Naciones Unidas]

Asunto: Noticias

Hola:

Por favor, lee el siguiente artículo, es muy importante:

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A otro miembro de la redacción de AP]

Associated Press

San Diego

Mobile [borrado]

Se trataba de phishing, una forma de ataque informático que consiste en intentar adquirir información confidencial (una contraseña, datos bancarios…) de forma fraudulenta a partir de un mensaje aparentemente fiable que nos invita a descargar un documento o abrir un link.

El ataque fue técnicamente sencillo, pero bien elaborado. Los piratas informáticos enviaron una decena de correos electrónicos falsos a otros tantos miembros de la redacción de la agencia de noticias. El mensaje cuidaba muy bien los detalles para dar sensación de verosimilitud: parecía enviado por un funcionario de Naciones Unidas que realmente existía e invitaba a abrir el enlace a una noticia de The Washington Post, cuya URL no despertaba ninguna sospecha.

Sin embargo, el hipervínculo no llevaba a ningún artículo sino a un sitio que replicaba el inicio de sesión para Outlook, la plataforma de

correo electrónico que utilizan los reporteros de AP. Esto no levantó ninguna sospecha en los periodistas, que creían que su sesión se había cerrado de forma involuntaria. Así que volvían a meter sus datos (ID de usuario y contraseña) en lo que creían que era un cuadro de diálogo del programa de correo. Sin embargo, lo que realmente estaban haciendo era dando acceso al autodenominado Ejército Electrónico Sirio (Syrian Electronic Army) a su sistema. A los cracker les había llevado menos de diez minutos conseguir la información.

La cuestión no era solo que hubieran obtenido las claves para controlar la cuenta oficial de Twitter: "El verdadero problema no es que se tuiteó algo, es que ahora sabían la lista de contactos de todos los rebeldes sirios que estaban enviando correos electrónicos a los periodistas occidentales", según declaró el experto Kevin Mandia a Business Insider (Ingersoll, 2013).

El episodio abrió un encendido debate sobre si la falsificación del tuit podía considerarse o no una agresión terrorista (Fisher, 2013). ¿Este asalto del Ejército Electrónico Sirio a AP debía contemplarse como un ataque informático entre tantos, era vandalismo, o se trataba de una acción de ciberguerra?

Cuando hablamos de "ciberguerra", en general, estamos aludiendo a muchos factores distintos a la vez. En los enfrentamientos bélicos actuales, y aún más en los futuros, la tecnología va a intervenir de formas variadas: unas veces como arma, otras como campo de batalla y otras como soporte de nuevas tácticas y estrategias. Es decir, bajo el paraguas de la idea "ciberguerra" entran en juego muchos elementos (nuevos dispositivos de ataque, nuevos blancos y objetivos, nuevos actores…), y no siempre participarán todos a un tiempo. En sentido estricto, "ciberguerra" sería cualquier conflicto bélico en el que el ciberespacio y las tecnologías de la información sean el escenario principal. Sin embargo, lo más frecuente serán los conflictos híbridos en los que se combinen entornos (y daños) reales y virtuales. Más aún si tenemos en cuenta que cada vez resulta más complicado separar ambas escenas. Un ataque informático, por ejemplo, tiene ya importantes consecuencias en el terreno físico, y esa capacidad "destructora" irá a más. Y los militares también tienen claro que cualquier conflicto armado, por convencional que

pueda parecer, tendrá su desarrollo “paralelo” en el ciberespacio (González, 2013).

Una dificultad añadida para precisar de qué estamos hablando es que conceptos como “ciberseguridad”, “ciberterrorismo”, “ciberespionaje” o “cibercrimen” se encuentran en la esfera de lo que puede entenderse como “ciberguerra” y, en ocasiones, incluso se usan indistintamente, lo que no es del todo riguroso (Singer y Friedman, 2014). También las fronteras se difuminan cuando se pretende catalogar la novedad de lo que ocurre, porque lo más desconocido, o tecnológicamente revolucionario —como los insospechados avances en inteligencia artificial que van a llegar—, convivirá con amenazas tan antiguas como la propia informática —por ejemplo, las técnicas clásicas de los ciberataques: desde el software malicioso a la ingeniería social—, aunque, eso sí, con un alcance hasta ahora desconocido.

¿Cuáles son, entonces, las claves de estos nuevos conflictos, que se nos presentan como la gran amenaza global, sobre los que sabemos muy poco y de los que nuestros gobiernos nos informan aún menos? Para aproximarnos a lo que es la “ciberguerra” podemos fijarnos en cinco elementos que han cambiado respecto a las contiendas tradicionales: el campo de batalla (ahora es el ciberespacio); el formato (estaríamos en una guerra en red); los agentes que participan (ya no son solo los ejércitos de los países); las formas de luchar (nuevas modalidades de ataque y nuevas armas), y los cambios en las tácticas y estrategias.

Estas cinco claves, que pueden servir para explicar qué es la ciberguerra, las desarrollamos en detalle en los siguientes apartados.

Nuevo territorio: el ciberespacio

Si las guerras se venían definiendo por el área geográfica en la que tenían lugar, en el caso de la "ciberguerra" este ámbito es el ciberespacio. En él desarrollamos buena parte de nuestra vida y realizamos operaciones tan sensibles como volcar nuestra intimidad o gestionar nuestros ahorros. Sin embargo, todavía rodea al término un halo de futurismo y ciencia-ficción. Fue precisamente en este género donde el concepto se popularizó. Se atribuye su empleo por primera vez al autor ciberpunk William Gibson (2007), en su novela Neuromante, publicada originalmente en 1984. Este autor utilizó el término "ciberespacio" para referirse a una realidad simulada que se encontraba implementada dentro de los ordenadores y de las redes digitales de todo el mundo.

Más tarde, en 1995, en el Foro de Davos, John Perry Barlow pronunció su famosa "Declaración de Independencia del Ciberespacio", donde se reivindicaba la autonomía de este lugar frente a las reglas y convenciones del mundo físico. Un texto que, al recuperarlo ahora, nos enfrenta a la libertad que, en menos de dos décadas, se ha perdido. Se trata de un documento, que, además de constituir una declaración de principios, incluye algunos rasgos claves de esta nueva frontera:

Gobiernos del Mundo Industrial, desgastados gigantes de carne y acero: vengo del ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido que nos dejéis en paz en el pasado. No sois bienvenidos entre nosotros. No tenéis ninguna soberanía sobre el lugar donde nos reunimos.

[…] No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra

cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

[…] El Ciberespacio está formado por transacciones, relaciones y pensamiento en sí mismo, que se extiende como una onda estacionaria en la telaraña de nuestras comunicaciones. El nuestro es un mundo que está a la vez en todas partes y en ninguna, pero no está donde viven los cuerpos físicos […].

Más allá de la utopía o la ficción, el ciberespacio es muy real. Por eso, que se le defina de un modo u otro puede tener una gran repercusión, como advierte Schneier:

Si enmarcamos esta discusión como una discusión de guerra, entonces lo que se hace cuando hay una amenaza de guerra es llamar al Ejército y se obtiene una solución militar. Si se piensa en estas amenazas en términos de delincuencia, se obtienen soluciones policiales. La forma en que enmarcamos este debate, la forma en que hablamos sobre él; la forma en que se dan los titulares, determina qué tipo de soluciones queremos[14].

En el campo de la Defensa, precisar el concepto de ciberespacio no ha sido una cuestión trivial. En él, se le considera un dominio militar más a sumarse a los clásicos de “tierra, mar, aire y espacio”[15]. En este contexto, el ciberespacio sería aquel “dominio global y dinámico compuesto por las infraestructuras de tecnologías de la información (incluido Internet), las redes, los sistemas de información y telecomunicaciones” (Quintero Villaroya y Estrada Matamala, 2014).

Ese carácter dinámico (¿quién sabe lo que será mañana el ciberespacio?) y global explica la complejidad de este nuevo campo

de batalla. Pero también otras características de este terreno virtual que suponen retos en una guerra, como lo relativo a las fronteras y a la soberanía o a la presencia distribuida de los agentes que participan.

El ciberespacio, según esta idea, tendría tres características que hay que tener en cuenta: se trata de un ámbito artificial creado por medios informáticos; se caracteriza por el uso de la electrónica y el espacio electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada; y es el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas webs, foros, servicios de Internet y otras redes (ibídem).

El Ejército norteamericano ha acometido en distintas ocasiones la tarea de especificar el concepto de ciberespacio. Una de sus definiciones recientes fue establecida por la Secretaría de Estado de Defensa en mayo de 2008, en un memorándum que recoge las conclusiones de un grupo creado específicamente para ello y que sigue la línea de una Directiva Presidencial previa sobre ciberdefensa desclasificada en 2014[16]. Según ese texto, el ciberespacio es "la red interdependiente de las infraestructuras de las tecnologías de la información, e incluye Internet, redes de telecomunicaciones, sistemas informáticos y los procesadores y controladores embebidos en industrias críticas. El uso común del término también se refiere al entorno virtual de información e interacciones entre personas". Posteriormente, en 2013, el Estado Mayor Conjunto de los Estados Unidos, en su documento "Cyberspace Operations" amplía esta definición para incluir "el contenido que fluye a través y por medio de estos componentes". Además, el documento incorpora la idea de las capas para explicar la interrelación entre el espacio físico y el ciberespacio: por ejemplo, los servidores de red son nodos que residen en dominios físicos (en un lugar geográfico concreto) y realizan funciones tanto en estos como en el ciberespacio. Lo mismo ocurre con las transmisiones de red wifi a través del aire, del espacio, e incluso bajo el agua.

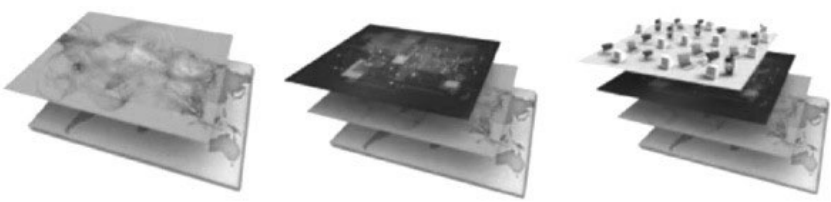
Merece la pena detenernos brevemente en la descripción de cada una de las capas para ver los problemas que pueden surgir en un

contexto de guerra, como la cuestión territorial o de responsabilidad de las acciones.

Figura 2

Las tres capas del ciberespacio según el Ejército de Estados Unidos

Capa de la red física Capa de la red lógica Capa de ciberpersonas



Fuente: Estado Mayor Conjunto de los Estados Unidos (2013).

Según esta idea, el ciberespacio consistiría en muchas redes diferentes que, a menudo, se superponen. La primera capa, la red física del ciberespacio, estaría formada, por un lado, por el medio geográfico y, por otro, por los componentes de la red a través de los que viajan los datos.

El medio geográfico es la ubicación en la tierra, aire, mar o espacio donde residen los elementos de la red. Y aquí se produce un contraste que debemos tener en cuenta en un escenario de guerra: mientras que las fronteras geopolíticas “se pueden atravesar fácilmente en el ciberespacio a una velocidad cercana a la luz —dice el Estado Mayor norteamericano—, todavía hay cuestiones de

soberanía vinculadas a los dominios físicos".

Los componentes de la red, por su parte, serían el hardware, el software de los sistemas y la infraestructura (alámbrica, inalámbrica, enlaces cableados, enlaces EMS, vía satélite y óptico) que sostiene a la red y a los conectores físicos (hilos, cables, radio frecuencia, enrutadores, conmutadores, servidores y ordenadores).

La importancia de conocer cómo funciona esta infraestructura y qué consecuencias puede tener era fácil de ver con una herramienta (ahora en desuso) denominada Border Check, desarrollada por el hacker español "Lord Epsylon" y que mostraba el recorrido que hacen nuestros datos cuando estamos navegando por la red, es decir, "por qué servidores y cables pasan la información en busca de su destino y, por tanto, quiénes son los individuos, organizaciones y gobiernos que pueden modificarla, almacenarla o, simplemente, enrutarla de otra forma" (Gómez Delgado, 2013).

De esta manera permitía darse cuenta de una realidad de la que normalmente no somos conscientes: "Cómo las mismas conexiones a Internet, realizadas por diferentes usuarios, se realizan por rutas diferentes. Eso no es neutro. Y hay varios factores que hacen que así sea, como, por ejemplo, el lugar donde se encuentra el usuario físicamente (y el Gobierno que hay detrás) o la forma en la que el proveedor de servicios (ISP) ha conectado las redes y ha configurado las rutas, que, por cierto, generalmente se realizan mediante acuerdos comerciales de los que no se tiene constancia pública", explicaba Epsylon.

Y es que "la actual estructura y protocolos de Internet que permiten la comunicación de millones de personas y máquinas tienen un carácter descentralizado pero controlable, ya que los grandes routers basan, principal y teóricamente, la elección de las rutas por las que mandar la información en la velocidad (Algoritmo de Dijkstra). Es decir, si un router de Estados Unidos tiene una tecnología que permite mover mayor cantidad de datos por milisegundo, entonces muchísimas más veces será seleccionado por el resto de routers para que la información viaje por allí. Esto, una vez más, rompe la neutralidad de la red, ya que permite que los gobiernos de países con mejores infraestructuras puedan monitorizar, almacenar e incluso alterar los datos que viajan por las

infraestructuras que están dentro de las fronteras de su legislación (siempre y cuando esta lo permita)" (Andrades, 2013).

Esto nos lleva a lo que el Ejército norteamericano denomina "segunda capa", la de la red lógica, que consistiría en aquellos elementos de la red que están relacionados entre sí de una manera independiente de la red física. Un ejemplo sencillo es cualquier sitio web que está alojado en servidores de múltiples ubicaciones físicas.

Por último, la "capa ciberpersona" estaría formada por las personas, físicas y jurídicas, que actúan en la red. En esta capa se crean las representaciones digitales de los individuos y las entidades en el ciberespacio, utilizando las reglas que se aplican en la capa de la red lógica. Las ciberpersonas se relacionan incorporando datos biográficos o corporativos, correo electrónico y dirección(es) IP, páginas web o números de teléfono, entre otra información. Este nivel también presenta complejidades, como que un individuo pueda tener múltiples identidades cibernéticas y que una identidad cibernética pueda tener varios usuarios; la atribución de la responsabilidad o que "la orientación sea difícil —advierte el Ejército— porque la ubicación no reside en un único lugar físico sino en muchos virtuales, como redes sociales, webs o almacenamiento en la nube".

La guerra en red

¿Qué tienen en común las técnicas de propaganda del terrorismo islamista, los ataques informáticos (no reconocidos) de los ejércitos o las redes de ordenadores zombis que ejecutan órdenes dictadas a distancia? Todos ellos son manifestaciones del carácter "irregular" de las contiendas en este nuevo escenario. Bienvenidos a la ciberguerra de guerrillas.

Condicionada por el terreno —el ciberespacio—, los actores que intervienen —organizaciones, grupos o individuos distribuidos— y la "cultura" de la sociedad de la información, la ciberguerra no es un conflicto convencional: es una guerra en red. El concepto de "guerra en red" se refiere tanto a una forma de actuar como de organizarse (Arquilla y Ronfeldt, 1993 y 1996). Entra en esta categoría cualquier tipo de conflicto (bélico o no) desarrollado por organizaciones que adoptan estrategias en red (frente a estrategias convencionales y jerárquicas) aprovechando los recursos tecnológicos disponibles.

La tecnología es clave para el surgimiento de los conflictos en red: permite que individuos y grupos dispersos creen redes de cooperación para hacer frente a problemas transnacionales que asumen como comunes. No es algo exclusivo de ejércitos o guerrillas militares: "Las ONG han formado redes transnacionales de defensa en torno a objetivos compartidos, las empresas multinacionales han distribuido en red sus operaciones en todo el mundo y las organizaciones criminales y terroristas se han desplazado a formas en red más ágiles y resistentes", por mencionar algunos de los ejemplos más recurrentes usados para ilustrar el término. Las nuevas formas de protesta social (Tascón y Quintana, 2012) también responden a lo que los expertos de Rand bautizaron como "guerra en red".

En términos de Defensa, una guerra en red es una guerra asimétrica: conflictos entre naciones o grupos que tienen capacidades militares

y estrategias dispares. No existe un frente determinado, ni caben acciones militares convencionales, sino que se emplean tácticas atípicas como la implicación de la población civil o un uso intensivo de las acciones de propaganda. Frente al uso de recursos militares de forma abierta, alguno de los contendientes (en apariencia los más débiles, pero no necesariamente) "tratará de desgastar, debilitar y obtener ventajas actuando de forma no convencional mediante éxitos puntuales de gran trascendencia en la opinión pública, agotamiento de su adversario por prolongación del conflicto, recurso a métodos alejados de las leyes y usos de la guerra o empleo de armas de destrucción masiva. Todo ello con el objetivo principal de influir en la opinión pública y en las decisiones políticas del adversario", según explica el coronel español Antonio Cabrerizo (Tascón y Quintana, 2012; Cabrerizo Calatrava, 2012).

Se diferenciaría de un conflicto convencional, o simétrico, porque este "se produce entre fuerzas armadas de naturaleza similar, y en el que se usan los mismos modelos estratégicos militares. Este conflicto se caracteriza normalmente por el enfrentamiento abierto entre fuerzas regulares, una elevada intensidad y ritmo y una situación final que suele ser consecuencia directa del resultado del enfrentamiento militar" (Cabrerizo Calatrava, 2012).

Este carácter irregular de la ciberguerra abre el debate sobre si estas acciones no estarían más cercanas al terrorismo que a los conflictos bélicos tal como los conocemos, según defienden algunos expertos en seguridad informática, como Eugene Kaspersky, "descubridor" de buena parte de los ataques más sonados en la última década: "'Ciberguerra' es utilizado por muchos para describir la situación, pero ese término que implica que hay dos iguales —dos enemigos conocidos enzarzados en combate— es anticuado. Con los ataques de hoy, en los que no se tiene ni idea ni quién lo hizo, ni cuándo van a atacar de nuevo, no es ciberguerra, sino ciberterrorismo" (Shamah, 2012).

Nuevos actores: quién es quién en la ciberguerra

Mientras que en la guerra tradicional los únicos actores son los ejércitos, en la ciberguerra esto cambia por completo. Junto a protagonistas tradicionales como los Estados, van a aparecer grupos emergentes con capacidad de participar en este tipo conflictos. El carácter de guerra en red de la ciberguerra va a dar ventaja a quienes adapten su organización y estrategia a esta nueva modalidad de enfrentamiento. Esto permite un amplio espectro de agentes con motivaciones y niveles de peligrosidad diferentes. Con todo, los gobiernos acumulan una gran capacidad de intervención y, de forma directa o indirecta, parecen estar detrás de la mayoría de las escaramuzas que se pueden catalogar como "ciberguerra". En cualquier caso, no conviene olvidar que uno de sus aspectos más problemáticos en este terreno es la atribución de un ataque. Lo más frecuente es que no pueda llegar a saberse con certeza quién es el último responsable (Schneier, 2005), más allá de deducciones a partir de indicios más o menos sólidos.

LOS ESTADOS

Hoy, por hoy, los gobiernos son los principales promotores de las batallas que, en el ámbito de la ciberguerra, se están librando: desde ataques informáticos contra blancos más o menos estratégicos, al desarrollo de nuevas ciberarmas, pasando por el ciberespionaje. Este último sería, para el Centro Nacional de Inteligencia español (CNI), la mayor ciberamenaza de la actualidad. Y, según este organismo, son precisamente los Estados quienes lo promueven: "Las evidencias permiten afirmar que, en significativas ocasiones, tales acciones han sido llevadas a cabo por servicios de inteligencia o departamentos de Defensa extranjeros, que siguen

invirtiendo importantes recursos en dotarse de capacidades de defensa y, también, de ataque" (Centro Criptológico Nacional, 2016).

Los Estados son también protagonistas por ser objeto, a su vez, de estas incursiones "con origen en otros Estados, interesados en obtener información de relevancia económica, geoestratégica o militar", según el CNI. Además, los países realizan ciberataques como una estrategia más dentro de los conflictos internacionales de los que son parte. Estos son algunos de los principales escenarios de esta ciberguerra entre Estados (Andrades, 2013; Zetter, 2015a):

Estados Unidos. Es el líder del ciberespionaje mundial: el alcance de la Agencia de Espionaje norteamericana (NSA) parece ser ilimitado, según los documentos filtrados por Edward Snowden (Quintana, 2014b; Greenwald, 2014)[17], que describen una vasta operación de piratería informática destinada a subvertir la infraestructura de Internet, según valoran los principales expertos en seguridad (Schneier, 2013a y 2013b).

Estados Unidos tiene capacidad de acceder a metadatos (quién se comunica con quién, desde dónde, en qué momento, con qué dispositivo, etc.) y contenidos (voz, texto e imágenes) de prácticamente cualquier comunicación digital (llamadas, correo, navegación). Pero no se trata solo de vigilancia masiva e indiscriminada y de rastreo online específico a objetivos "civiles" como activistas, políticos y periodistas. Estados Unidos ha desarrollado, asimismo, un gran potencial para el ciberataque. Su principal hito se sitúa en 2010, cuando lanzó, junto con Israel, el gusano Stuxnet contra Irán para sabotear el programa nuclear de ese país, lo que logró por un breve periodo de tiempo.

"Stuxnet sentó un precedente para la guerra cibernética, en la que los países lanzan ataques digitales para resolver disputas políticas", según la periodista de Wired, Kim Zetter, autora de un libro sobre este caso.

Además del desarrollo de ciberarmas como Stuxnet, Estados Unidos ha realizado otras actividades que ponen en peligro la seguridad

global en Internet[18], como la alteración de equipos, los ataques a los sistemas de cifrado y protocolos seguros (como el HTTPS que todos usamos en nuestras transacciones) (Quintana, 2015a), la explotación de vulnerabilidades no conocidas o el uso furtivo de las denominadas "puertas traseras" (Velasco, 2014; Peirano, 2016b). Junto con sus acciones mantiene una guerra cibernética contra "Estados enemigos" como Irán o Corea del Norte. Este último y sus instalaciones nucleares se han convertido en otro de los objetivos prioritarios, tanto de su vecino del sur como de Estados Unidos.

Uno de los episodios de esta tensión fue la entrada de hackers en las redes norcoreanas, aisladas del resto de Internet, "gracias a un despliegue de antenas wifi amplificadas que pudieron captar la señal y establecer un punto de entrada desde lugares próximos a la frontera", explica el informático forense Fran Andrades (2013). "La intrusión terminaría por afectar a diversas infraestructuras, aunque no alcanzará a ordenadores con información acerca del programa nuclear", cuenta. Como resultado, el norte declaró nulos los términos del armisticio entre ambas Coreas.

Estados Unidos mantiene entre sus prioridades estratégicas el "asalto" a las redes que dirigen el programa militar de Corea del Norte, según se desprende de los documentos estratégicos no clasificados del Ejército norteamericano, en los que afirman disponer "de una variedad de herramientas para el (ciber)ataque".

China. Ha estado detrás de algunas de las operaciones más sonadas de la historia de la ciberseguridad. Entre 2009 y 2011, logró hackear Google, RSA Security y otras compañías para obtener su código fuente y otros datos sensibles.

El caso de Google, bautizado como "Operación Aurora", fue descrito como un ataque sin precedentes por su sofisticación (Zetter, 2010d), al combinar cifrado, software furtivo —se emplearon una docena de programas maliciosos— y una vulnerabilidad no conocida de Internet Explorer. Detrás de esta operación estaría la negativa de Google de aplicar las cláusulas de censura que el Gobierno chino pretendía imponer al buscador, a pesar de sí haber hecho cesiones parciales.

El ataque contra la empresa de seguridad norteamericana RSA Security, que cuenta entre sus clientes con agencias gubernamentales, supuso el acceso a datos clave de uno de sus productos de autentificación y cifrado (Zetter, 2011b).

Otros de los puntos fuertes de China han sido los ataques de denegación de servicio o DDoS (hacer llegar a una web una sobrecarga de peticiones imposibles de procesar, por lo que el sitio aparece como "no disponible"; lo que coloquialmente se llama web "caída"). Un informe atribuía a China el 41 por ciento del tráfico global de estas acciones en 2012. "El crecimiento de estos ataques y la multiplicación de sus orígenes hacen que las estrategias de seguridad de empresas no directamente vinculadas a la red, como bancos y medios de comunicación, queden expuestas. La escalada en la complejidad evidencia cada vez más que sin un claro patrocinio y el respaldo de una infraestructura cada vez mayor no es posible llegar a la escala actual que adquieren estos ataques", según explica Andrades.

Más tarde, en 2014, China habría estado detrás de la violación de varias bases de datos de la Oficina de Administración de Personal norteamericana, en las que se robaron datos sensibles, incluyendo números de la Seguridad Social de más de 21 millones de personas.

Un caso que refleja la curiosa tensión entre Estados Unidos y China es el de Huawei, la empresa de telecomunicaciones líder del país asiático: mientras que en 2012 era acusada por una comisión del Congreso de mantener puertas traseras abiertas en sus routers para permitir el acceso a sus infraestructuras y un eventual espionaje (Gorman, 2012) (provocando la queja formal por parte de la embajada China), los papeles de Snowden desvelaron que era Estados Unidos quien mantenía una intensa actividad de espionaje hacia esta compañía (Appelbaum, 2013; Spiegel, 2014).

China, por su parte, "apenas reporta casos en los que su seguridad haya sido comprometida, a pesar de la constancia de que no dejan de sucederse casos en ambas direcciones. Así, el Ministerio de Defensa chino y otros sitios militares han llegado a contabilizar mensualmente un promedio de 144.000 a lo largo de 2012, de cuyo origen parece que un 62,9 por ciento partía de Estados Unidos, según una de las pocas informaciones suministradas" (Andrades,

2013). Una tensión bilateral que no impide que eventos públicos como el Foro de la Industria de Internet China y Estados Unidos "acojan calurosas declaraciones de intenciones en las que la colaboración entre ambos países contra el crimen y el espionaje online son la clave" (Andrades, 2013).

Reino Unido. Gran Bretaña, detrás de Estados Unidos, ocupa el segundo puesto en las actividades de ciberespionaje global. No en vano, ambos países lideran la denominada "Alianza de los Cinco Ojos"[19] (que también integran Nueva Zelanda, Australia y Canadá) y mantienen una más que estrecha colaboración.

Los documentos filtrados por Snowden han demostrado que Reino Unido hackeó los cables submarinos de Yahoo y de Google para acceder a las comunicaciones sin cifrar que transmiten. Y no solo a los de estas empresas de Internet, sino también a los de las grandes compañías de telecomunicaciones. Entre sus proezas, el ataque en 2012 a la empresa de telefonía belga Belgacom para supervisar todo el tráfico móvil que pasa a través de sus routers. Una de sus actividades, descubierta recientemente y que muestra sin tapujos la verdadera cara de la ciberguerra de los Estados, es el "hackeo" a teléfonos y ordenadores de los refugiados y solicitantes de asilo que Reino Unido habría estado realizando desde 2013 (Sarabia, 2016).

Israel. También se encuentra entre los Estados más activos en el empleo de ataques informáticos como arma de guerra. Además de su actuación destacada en la creación y propagación de Stuxnet y otros ataques similares (Duqu y Flame), se cree que, en 2012, lanzaron el virus Wiper contra el Ministerio de Petróleo iraní y la compañía nacional de petróleo. El malware borró datos del disco duro y archivos del sistema, haciendo que las máquinas se bloquearan y obligando a Irán a desconectarlas de Internet (Erdbrink, 2012).

En 2014, Israel habría —supuestamente— atacado, con software espía, la firma de seguridad rusa Kaspersky Lab para obtener información de sus investigaciones sobre los ataques de este Estado. También habrían accedido a hoteles y centros de conferencias donde los miembros del Consejo de Seguridad de las Naciones Unidas se reunieron para negociar el programa nuclear de Irán. El

espionaje se centró en las negociaciones nucleares, en las que no participaba Israel, lo que parece apoyar esta teoría (Zetter, 2014c).

Israel, por su parte, también ha sido objetivo de este tipo de acciones. En los últimos años, hackers propalestinos han llevado a cabo ciberataques contra sitios web israelís gubernamentales, de aviación o de entidades financieras (Lake, 2012; Kershner, 2013). Una de estas campañas, reivindicada por Anonymous, OpIsrael, supuso el borrado de más de 1.000 sitios web israelíes, incluyendo dominios web del Gobierno como los del Mossad, el Departamento de Policía de Tel Aviv o el Ministerio de Defensa de Israel. La campaña se llevó a cabo mediante ataques de denegación de servicio, secuestro y filtraciones de bases de datos, dominio de paneles de control y desfiguraciones de webs. En algunos casos, las fuerzas de seguridad de Israel respondieron con contraataques focalizados en sitios web de Hamas.

A principios de 2016, atacantes informáticos paralizaron la red eléctrica de Israel, según el Gobierno. La caída del suministro coincidió con un gran aumento en el consumo de energía por la bajada de las temperaturas (Khandelwal, 2016).

Corea del Norte. En 2014, Sony Pictures Entertainment fue objeto de un aparatoso ataque[20]*. El 24 de noviembre, un grupo de hackers autodenominados "guardianes de la paz" (GOP) filtraron datos confidenciales del estudio de cine Sony Pictures Entertainment. Los datos incluían información personal sobre los empleados y sus familias, correos electrónicos entre empleados, información sobre los salarios de los ejecutivos de la empresa y copias de películas inéditas, entre otra información. Estados Unidos atribuyó la acción a Corea del Norte y aplicó sanciones económicas adicionales contra el país y funcionarios específicos.*

En 2013, los equipos de Corea del Sur fueron alcanzados por una bomba lógica (una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta que, al cumplirse una o más condiciones preprogramadas, se ejecuta) que causó la eliminación de datos e impedía el reinicio de los equipos. Dos empresas de medios de difusión y al menos tres bancos se vieron afectados. Corea del Sur culpó a Corea del Norte del ataque, pero nunca se ha producido una evidencia sólida.

Estos ataques han servido para que Estados Unidos y Corea del Sur establezcan las bases para colaborar en un eventual escenario de conflicto en la red. ¿Qué supone este acuerdo? Que “las próximas intrusiones en el sistema del norte serán ya confirmadas sin excusa, como métodos de ‘defensa’”, según Andrades.

Irán. En 2012, Irán —supuestamente— lanzó un virus llamado Shamoon contra los ordenadores del conglomerado de petróleo saudí Aramco. Las autoridades estadounidenses culparon a Irán del ataque, pero nunca presentaron pruebas. Shamoon borró datos de unas 30.000 máquinas y destruyó archivos del sistema, dejándolas inoperativas. Entre 2011 y 2012, mediante la denominada Operación Ababil, Irán lanzó una serie de ataques de denegación de servicio contra entidades financieras de Estados Unidos. Los autodenominados “combatientes cibernéticos de Izz Ad-Din Al-Qassam” (Cyber fighters of Izz Ad-Din Al-Qassam) se atribuyeron la responsabilidad. El grupo anunció los ataques del 18 de septiembre de 2012 en Pastebin (una aplicación web que permite a sus usuarios subir pequeños textos, generalmente ejemplos de código fuente, pero usada también por hacktivistas, como Anonymous, para difundir sus acciones).

Los objetivos incluyeron la Bolsa de Nueva York y los principales sitios de banca online. En tres oleadas de ataques, los consumidores fueron informados de la imposibilidad de llevar a cabo transacciones en línea en más de una docena de bancos, incluyendo Wells Fargo & Co (WFC.N), Citigroup Inc (CN), JPMorgan Chase & Co (JPMN) y Bank of America Corp (BAC.N).

Los ataques afectaron al rendimiento de los equipos, pero sin daños a largo plazo, según se informó en su momento para tratar de minimizar su impacto. Sin embargo, el coste económico fue elevado para las compañías afectadas, que tuvieron que destinar millones de dólares a defenderse de los piratas informáticos y restaurar el servicio (Menn, 2013).

A pesar de la reivindicación de los combatientes cibernéticos de Izz Ad-Din Al-Qassam, algunos funcionarios estadounidenses afirmaron que Irán estaba detrás de la acción, buscando vengarse por el ciberataque de Stuxnet y las sanciones de las Naciones Unidas. Una

tesis que se apoyaba en el tamaño del ataque: 65 gigabytes de tráfico por segundo, mientras que un ataque hacktivista típico de denegación de servicio sería de menos de 2 gigabytes por segundo (Gonsalves, 2012).

Más tarde, los documentos desvelados por Snowden revelaron que Estados Unidos admitía haber contribuido a que Irán se iniciase en la ciberguerra (Greenwald, 2015), algo de lo que ya habían advertido los expertos en seguridad informática cuando el virus Stuxnet fue descubierto: que los adversarios de Estados Unidos aprenderían de ello y desarrollarían técnicas similares contra este país y sus aliados (Zetter, 2015a).

El documento filtrado por Edward Snowden revelaba que la NSA temía lo mismo y que Irán ya podía estar haciendo exactamente eso. El escrito de la NSA, fechado en abril de 2013, sugería que ataques como Stuxnet, Flame y Duqu (todos ellos creados por Estados Unidos) no solo habrían invitado a contraataques de adversarios, sino que también enseñaban nuevas técnicas y herramientas, lo que les habría permitido aumentar la sofisticación de su respuesta. Irán, dice el documento, "ha demostrado una clara facultad para aprender de las capacidades y acciones de los demás".

El documento, un informe preparatorio de una reunión entre el director de la NSA y la agencia de espionaje británica Government Communications Headquarters (GCHQ), no mencionaba el ataque de Stuxnet por su nombre, sino que se refería a él como "los ataques occidentales contra el sector nuclear de Irán". Además, también se afirma que Irán habría aprendido de un ataque previo que afectó a su industria petrolera, cuya técnica habría luego replicado en su acción contra el conglomerado saudí Aramco. La referencia alude al virus Wiper, "una pieza agresiva y destructiva de malware" que se dirigió contra los equipos del Ministerio de Petróleo iraní y la compañía nacional de petróleo, en abril de 2012, y que se atribuye a Estados Unidos o Israel (Perlroth, 2012; Zetter, 2012; Mills, 2012).

Wiper fue "diseñado para destruir todos los archivos tan rápidamente como sea posible, lo que puede incluir varios gigabytes en un momento", según los investigadores de Kaspersky Lab que examinaron los discos duros destruidos. Wiper fue el primer ataque

conocido de destrucción de datos de este tipo.

Rusia. En 2007, Rusia llevó a cabo el primer ciberataque Estado-Estado contra Estonia. Aunque la OTAN más tarde minimizaría el episodio, calificándolo de "ciberturba", parece que se trató del primer ensayo para medir la eficacia de las botnets: red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. Al respecto, Andradres (2013) explica lo siguiente:

Por aquel entonces, el país báltico era una de las naciones de mayor penetración digital de Occidente. Diversos sistemas fundamentales, entre los que destacaban el sistema bancario y las infraestructuras públicas, desde saneamiento hasta los mismos semáforos, fueron bloqueados durante cerca de dos semanas a consecuencia de la retirada de un monumento identitario para la población rusa que habita el país. Expertos de la OTAN tendrían que acudir para tratar de hacer cesar dicho ataque, cuyo origen se ubicaría finalmente en la Federación Rusa.

En aquel momento el ataque no fue reconocido, pero "especulaciones posteriores apuntarían a una suerte de 'encargo' a hackers con capacidades de movilizar enormes botnets para llevar adelante estos", agrega Andrades.

Más tarde, en 2014, Rusia hackeó —supuestamente— el Departamento de Estado y la Casa Blanca. Los atacantes tuvieron acceso a los correos electrónicos no clasificados del presidente Obama, así como detalles no públicos acerca de su horario.

Un año después, en 2015, Rusia es señalada por Francia por haber hackeado la cadena de televisión francesa TV5Monde, aunque el ataque se lo atribuyó un grupo autodenominado "CyberCaliphate". Durante varias horas, los piratas informáticos interrumpieron la emisión de los 11 canales de la cadena y publicaron mensajes de apoyo al extremismo islamista en cuentas de redes sociales del

canal de televisión (Reuters, 2015a).

Otros Estados. India y Pakistán también han protagonizado diversas escaramuzas de ciberguerra. En marzo de 2012, el ministro indio para la Tecnología de la Información y Comunicaciones reveló, en una respuesta escrita a una pregunta parlamentaria, que 112 sitios web del Gobierno habían sido comprometidos en solo dos meses (de diciembre de 2011 a febrero de 2012). La mayor parte de los incidentes eran desfiguraciones de web y muchos de los atacantes parecían ser originarios de Pakistán. En los últimos años, además, han sufrido diversos incidentes de gravedad variable de robo de información.

Pakistán, por su parte, también ha sido objeto de ciberataques, como el sufrido en 2013 en la web de la compañía telefónica Telenor-Pakistan por el grupo de hackers indio Cyberhax0rs.

En cuanto a América Latina, en el terreno de la "ciberguridad", según los estudios que han analizado la expansión de ataques en el continente, parece que la actividad allí estaría más ligada a la ciberdelincuencia (por ejemplo, operaciones de blanqueo de dinero) que a escaramuzas de ciberguerra (Igarape Institute-The SecDev Foundation, 2012). Una excepción sería el malware denominado "Machete", un software espía que afectó a diplomáticos y miembros de varios gobiernos de la zona.

Asimismo, debemos mencionar la primera firma de un tratado de "no agresión" con armas informáticas suscrito por Brasil con Rusia.

GRUPOS TERRORISTAS

Según los servicios de inteligencia, el ciberterrorismo no sería una amenaza inminente: "Aunque la peligrosidad potencial de las acciones atribuibles al ciberterrorismo sigue creciendo, no puede afirmarse que, en la actualidad, represente una grave amenaza, especialmente por las limitadas capacidades técnicas que se han

observado en sus despliegues", afirma en su informe anual sobre ciberamenazas el Centro Criptográfico Nacional (2016), organismo adscrito al CNI.

Ciberyihadismo. En este ámbito hay que destacar la actividad del ciberyihadismo y los grupos yihadistas: "En 2015 ha aparecido una nueva amenaza: el ciberyihadismo, que, usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra, constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años", anticipa el Centro Criptográfico Nacional.

También en esa línea, el experto Fran Andrades (2013) comenta que "podemos afirmar que el yihadismo internacional ha comenzado a ver cómo la actividad en la red puede ser empleada más allá de fuente de reclutamiento y comunicación entre sus miembros. Así, grupos como la ciberguerilla Izz Ad-Din Al-Qassam han comenzado a emplear metodologías muy similares a las que emplean grupos como Anonymous para realizar sus acciones en la red".

Un factor que hay que tener en cuenta, del que advierte el Centro Criptográfico Nacional, es la creciente capacidad de acción que cabe esperar de estos grupos: "Las importantes vías de financiación de estos grupos (al socaire de Daesh) hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento, sus ataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructura" (ibídem).

Los ataques recientes más destacados han sido: "Uso de código dañino (por ejemplo, en Siria se detectaron ciberataques para obtener datos sobre posiciones de los objetivos locales); ataque a sitios web; instrucciones para el uso de una herramienta de acceso remoto (RAT14) para el control de equipos; ataques a redes sociales para la obtención de información y ataques de 'phishing' para

obtener datos de tarjetas de crédito y obtener información" (ibídem).

Del 'Cibercalifato' al 'Cibercalifato Unido'. El Cibercalifato (Cyber Caliphate) es un grupo de atacantes informáticos que, en los últimos años, ha venido reivindicando su vinculación y apoyo al extremismo islámico. Una de sus acciones más "sonadas" fue el control de las cuentas en redes sociales del Mando Militar norteamericano (@centcom, en Twitter) en enero de 2015.

El atacante que supuestamente la llevó a cabo, un hacker de Birmingham de 21 años que en 2012 pasó seis meses en prisión por haber obtenido y publicado datos personales de Tony Blair, miembro del grupo TeaMp0isoN, llamado Junaid Hussain (Moore, 2015), fue matado por un dron dirigido por el Ejército norteamericano a finales de agosto de 2015, después de accionar en su teléfono un enlace malicioso que informaba de su ubicación exacta (Reuters, 2015b; McCarthy, 2015; Cartledge, 2015; Murphy, 2015; Simpson, 2015).

En realidad, no podía hablarse del Cibercalifato como grupo, pues la impresión era que se trataba de acciones más bien aisladas, con escasos miembros y poca coordinación. No obstante, esto podría cambiar con el anuncio realizado por grupos yihadistas online de crear una especie de unidad de acción cibernética autodenominada United Cyber Caliphate (UCC): "A través de una serie de mensajes compartidos en las redes sociales y en varios chats de Telegram, el grupo de piratas informáticos ha anunciado la creación de una gran unidad de piratas que, a partir de ahora, pasará a llamarse UCC, acrónimo de United Cyber Caliphate. Este nuevo grupo estará formado a partir de piratas informáticos de otros grupos a favor del terrorismo, todos pertenecientes a ISIS, como el Cyber Caliphate Army (CCA), Sons Caliphate Army (SCA) y el Kalacnikov.TN (KTN)"[21].

Sin embargo, por el momento, como estiman los servicios de inteligencia (Centro Criptológico Nacional, 2016), no parece que, a pesar de esta anunciada acción coordinada, supongan un riesgo inminente, pues la capacidad técnica demostrada hasta ahora es

más bien limitada. Así lo demuestran las acciones llevadas a cabo por tales grupos hasta el día de hoy, más orientadas a la propaganda (con acciones como desfiguraciones de webs) que a un daño de alcance concreto. Una monografía publicada a finales de abril de 2016 incidía en la misma idea del estado incipiente de esta ciberamenaza: unos grupos más preocupados por el impacto mediático de sus acciones (como muestran los blancos elegidos y los ataques llevados a cabo, como el control de perfiles de redes sociales de cuentas con gran visibilidad como las de Cetecom o Newsweek[22]) que con capacidad de desarrollar herramientas que permitan ataques más avanzados: "Hasta el momento, los hackers pro ISIS parecen haber lanzado ataques principalmente contra objetivos del Gobierno, la banca y los medios de comunicación. Estos objetivos parecen ser no solo el centro de los ataques, sino también los que generan la mayoría de la publicidad. Sin embargo, estos ataques se mantienen en un nivel relativamente 'novato' y son en su mayoría acciones oportunistas" (Alkhouri, Kassirer y Nixon, 2016).

Una muestra de ello son las acciones que estos grupos se atribuyen y cuyos blancos han sido tan modestos como un instructor de baile japonés, una empresa de suelos laminados de Gales u otra de paneles solares de Inglaterra. También sorprendentes confusiones, como cuando, en febrero de 2016, anunciaron atacar a Google y en realidad causaron una desfiguración a la web Add Google Online, de la empresa india Always Say, que presta servicios de SEO (optimización de posicionamiento en buscadores) (Cuthbertson, 2016).

El impacto del 'contraterrorismo'. Por otro lado, el terrorismo posee, de forma indirecta, un efecto en la paz y libertad del ciberespacio a través de las leyes y medidas que los países ponen en marcha con la coartada de su supuesta prevención, por más que los hechos contradigan, una y otra vez, ese argumento. Una estrategia que ha sido cuestionada por las Naciones Unidas, por organizaciones internacionales como Amnistía Internacional, American Civil Liberties Union (ACLU), Electronic Frontier Fundation (EFF) o, en España, la Plataforma en Defensa de la Libertad de Información (PDLI) (Quintana, 2015b).

La “lucha contra el terrorismo” se ha convertido en el nuevo comodín del populismo conservador, capaz de justificar cualquier legislación una vez modelada oportunamente la opinión pública. La realidad ha demostrado que la mayor parte de las líneas de actuación que se han anunciado públicamente han terminado por tener un empleo bien distinto. Las diversas unidades surgidas a partir de la Patriot Act, después del 11S, demostraron una escasa eficacia a pesar de la ingente cantidad de recursos destinados a estas. El espionaje del activismo dentro de los propios Estados Unidos ha terminado por ser una de las mayores actividades de dichos grupos. En este sentido, la ciberyihad parece ser el placebo necesario para mantener una tensión pública lo bastante asustada como para comulgar con una sustracción de derechos de otro modo intolerable (Andrades, 2013).

Grupos de hackers (crackers)

En ocasiones, promovidos por los Estados y, en otras, con fronteras difusas con el hacktivismo o la delincuencia informática, nos encontramos con los grupos de atacantes informáticos (crackers) organizados bajo una identidad digital. A continuación, haremos una breve descripción de algunos de los más conocidos o activos.

Los pioneros: Legion of the Underground. En diciembre de 1998, un grupo autodenominado “Legion of the Underground” lanza una declaración de ciberguerra contra China e Irak por sus vulneraciones de los derechos humanos a través de un comunicado (en el que se mencionan a sí mismos en tercera persona) que difunden online y en una “rueda de prensa” que tiene lugar en un canal IRC[23]. Bajo el título “Declarada la guerra a China e Irak”, el grupo Legion of the Underground manifestó lo siguiente:

En una discusión acalorada y emocional, Legion of the Underground declaró la ciberguerra a la infraestructura de la información de China y de Irak anoche. Citaron abusos graves de los derechos civiles por parte de los gobiernos de ambos países, así como la reciente condena a muerte de dos ladrones de bancos en China y la producción de armas de destrucción masiva por parte de Irak como las razones de su indignación.

Citando el derecho del pueblo a gobernarse a sí mismo contenido en la "Declaración de Independencia" y afirmando que el Gobierno de Estados Unidos probablemente quedará de brazos cruzados mientras estas atrocidades ocurren en otros países, Legion of the Underground llama a la destrucción completa de todos los sistemas informáticos en China e Irak.

"¡El Gobierno controla lo que entra en nuestras bocas, no le dejemos hacer lo mismo con lo que sale!", dijo un miembro de Legion of Underground durante una conferencia de prensa llevada a cabo en el IRC el lunes por la noche.

Legion of Underground mencionó asimismo que podrían recurrir a la ayuda de los Hong Kong Blondes (HKB), un grupo bien conocido por el intento de provocar el caos en las interconexiones de las redes de China desde el interior de la cortina de hierro. Los HKB fueron capacitados y asistidos, hasta hace poco, por el infame grupo de hackers Cult of the Dead Cow.

Legion of Underground ganó notoriedad el pasado octubre al desfigurar el sitio web de la organización de derechos humanos china (Chinese Human Rights) un día después de que se pusiera en línea

[24].

Este manifiesto provocó la reacción de los principales grupos hackers de entonces (2600, The Chaos Computer Club, The Cult Of The Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack, Pulhas y T0xyn), que difundieron un comunicado conjunto en condena. El texto posee un gran valor, pues refleja la visión de los hackers pioneros contra los ataques informáticos como forma de activismo: "No deis soporte a ningún acto de 'ciberguerra'; mantened las redes de comunicaciones vivas, son el sistema nervioso de nuestro planeta", decían.

Los grupos de hackers 2600, The Chaos Computer Club, The Cult of the Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack, Pulhas y T0xyn sienten la necesidad de comentar el reciente anuncio de un grupo que se hace llamar "Legion of the Underground".

Legion of the Underground ha declarado que tratarán de dañar y sabotear la infraestructura del ciberespacio de Irak y China. Citan los problemas con los derechos humanos en esos países como la causa de esta acción.

Aunque podamos estar de acuerdo con Legion of the Underground en que las atrocidades en China e Irak deben terminar, estamos en desacuerdo con los métodos que propugnan. Estos son cortos de miras y potencialmente contraproducentes. No se puede esperar legítimamente mejorar el libre acceso de un país a la información tratando de inhabilitar sus redes de datos.

Sin duda, la situación de los derechos humanos en China, Irak y muchos otros países de este planeta es pésima. El hacktivismo — usar las habilidades y herramientas de hacking para apoyar causas progresistas— puede ser, en algunos casos, a ojos de algunos de los

abajo firmantes, una manera legítima de atraer la atención pública a estos problemas.

Pero nos oponemos radicalmente a cualquier intento de usar el poder del hacking para amenazar o destruir las infraestructuras de comunicación de cualquier país, por ninguna razón. Declarar la "guerra" contra alguien, cualquier grupo de personas o nación es un acto totalmente deplorable. Lo único que hace es reducir al hacker al mismo nivel del grupo o país que está atacando. Esto no tiene ninguna relación con el hacktivismo o las éticas del hacker, y no es nada de lo que ningún hacker deba sentirse orgulloso.

Los gobiernos de todo el mundo están tratando de establecer el ciberespacio como el nuevo campo de guerra para sus conflictos artificiales. Lo que Legion of the Underground ha hecho es legitimar inadvertidamente estos propósitos. Si los hackers se establecen como armas, el hacking en general se verá como una acción de guerra. Y los mismos hackers serán vistos, sin ninguna duda, como objetivos legítimos para los países contendientes.

Desde nuestro punto de vista, Legion of the Underground está haciendo cosas que los gobiernos del mundo no quieren hacer pública u oficialmente. Los preparativos para la "guerra de la información" están, en Estados Unidos, y en cualquier otra parte, en un punto en que son necesarios casos "reales" para justificar los fondos asignados.

Legion of the Underground está proporcionando ahora este caso real. Creemos que debería investigar cuidadosamente si la idea de declarar la "guerra" a China e Irak no fue dada por alguien con intereses distintos a los de defender el problema de los derechos humanos.

Los firmantes piden a todos los hackers del planeta que rechacen todo aquello relacionado con dañar las infraestructuras de información de cualquier país. No deis soporte a ningún acto de "ciberguerra"; mantened las redes de comunicaciones vivas, son el sistema nervioso de nuestro planeta.

Todos los hackers y grupos de hackers están invitados a firmar (HackStory, s. f.; D'Amico, 1999).

Syrian Electronic Army. Cuenta Lorenzo Franceschi-Bicchierai, periodista de Motherboard, que el 19 de noviembre de 2013, Dan Layman estaba hablando por teléfono con el FBI cuando recibió un correo electrónico extraño. "Le estamos viendo", leyó. Era un mensaje remitido por admin@fbi-useless.gov, una dirección falsa. "Nadie le ayudará. Todos vosotros vais a caer", continuaba el mensaje.

Layman, portavoz de un grupo de lobby de apoyo a opositores al Gobierno sirio (Syrian Support Group), acababa de ser hackeado. Formaba parte de una campaña de ciberataques puesta en marcha por el Syrian Electronic Army, un grupo de crackers partidarios de Bashar al-Assad que apareció online por primera vez en 2011.

Entre sus técnicas se encontraban el spamming (correo basura), desfiguraciones de webs (defacement), malware, phishing (mensajes de correo maliciosos) y ataques de denegación de servicio dirigidos contra grupos políticos de la oposición, medios occidentales o grupos de derechos humanos. También ha hackeado sitios web del Gobierno en Oriente Medio y Europa, así como de contratistas de Defensa de Estados Unidos.

A principios de 2015, una monografía sobre este grupo de la empresa de ciberseguridad FireEye reveló que, entre otras acciones, los hackers habían atacado los ordenadores de la oposición siria, robado gigabytes de comunicaciones secretas y planes de batalla. Asimismo, los hackers infectaron los equipos de la oposición con

malware mientras mantenían conversaciones por Skype y sesiones de chats en las que se discutía de planes de guerra y logística. Frecuentemente, Utilizan malware del tipo keylogger, una herramienta específica diseñada para registrar las pulsaciones en el teclado de un equipo. Gracias a este programa, los delincuentes pueden robar un gran volumen de información confidencial sin que la víctima se percate de ello. Con esta táctica, los hackers han robado cientos de documentos y casi 31.107 conexiones a sesiones de chat de Skype. Los datos robados incluyen información militar, información política, actividades humanitarias y financiación, información personal sobre los refugiados, relaciones con medios de comunicación.

Lazarous Group (Grupo Lázaro). Este grupo, de identidades cambiantes (Guardians of Peace[25] o Whois Team[26], entre ellas), parece haber constituido en realidad una red de grupos. Es conocido, principalmente, por ser responsable del ataque a Sony Pictures Entertainment en 2014 y por sus ofensivas contra bancos y entidades de radiodifusión dl Seúl en 2013 (Operación Dark Seul y Operación Troy), aunque sus primeras acciones se remontan a 2007.

Fue "desenmascarado" a principios de 2016 en la llamada Operación Blockbuster (Novetta, 2016)[27], llevada a cabo por un consorcio de empresas de seguridad liderado por Novetta y Kaspersky (Guerrero-Saade, Raiu y GReAT, 2016). La investigación reveló que había participado en campañas militares de espionaje y sabotaje, en operaciones contra instituciones financieras, medios de comunicación y empresas de fabricación.

Para sus ataques, Lazarous Group ha creado programas maliciosos como Hangman (2014-2015) y Wild Positron (también conocido como Duuzer, 2015). La mayoría de los equipos infectados se encontraban en Corea del Sur, India, China, Brasil, Rusia y Turquía. La investigación les presenta como "adictos al trabajo": según Kaspersky, sus últimas jornadas de trabajo se prolongaban durante 15 y 16 horas. "Lazarous Group es probablemente el grupo APT (Amenaza Persistente Avanzada) más trabajador entre todos los conocidos por nosotros", aseguran.

Dos terceras partes de los archivos ejecutables elaborados por Lazarous incluyen elementos que son típicos para los usuarios de habla coreano. Siguen activos en la actualidad.

Dragonfly. El grupo Dragonfly parece haber estado en funcionamiento al menos desde 2011. Inicialmente, se centró en atacar empresas de Defensa y aviación de Estados Unidos y Canadá. Más tarde, a principios de 2013, cambió su blanco a empresas de energía. Capaz de lanzar ataques a través de varios vectores diferentes, su más ambiciosa campaña de ataque infectó una serie de sistema de control industrial (ICS) de proveedores de equipos, dañando su software con un tipo de acceso remoto troyano (Haley, 2014). Según Symantec (2014), ese malware "dio a los atacantes acceso completo a los sistemas en los que se había instalado este software. Si bien esto permite a los atacantes llegar a las organizaciones objetivo con el fin de llevar a cabo actividades de espionaje, muchos de estos sistemas estaban utilizando programas ICS para controlar infraestructura crítica, tales como oleoductos y redes de energía. Si bien no se vio ciberespionaje en estos ataques, no hay duda de que los atacantes tenían la capacidad y podrían haber puesto en marcha este tipo de acciones en cualquier momento. Quizás eligieron esperar y fueron interrumpidos antes de poder seguir adelante".

Waterbug-Turla. El grupo denominado Waterbug (por Symantec) o Turla (según Kaspersky) es el nombre dado a los actores que utilizan las herramientas de malware Trojan.Wipbot (también conocido como Tavdig y Epic Turla) y Trojan.Turla, y cuyas acciones se han dirigido sistemáticamente contra gobiernos, embajadas, centros de enseñanza y de investigación. También se les conoce como Carbon, Uroburos y Snake. Se cree que llevan activos desde al menos el año 2005. Es probable que el grupo fuera responsable del caso Agent.btz: el ataque al Mando Central de Estados Unidos de 2008 que, según los informes, dio lugar a una operación de limpieza de casi 14 meses. Este grupo ha abordado con éxito y ha comprometido más de 4.500 ordenadores en más de 100 países. Es probable que el malware detectado en los equipos de las víctimas (las variantes de Trojan.Turla y Trojan.Wipbot) haya sido desarrollado por o para el grupo. Trojan.Turla posee cuatro

subversiones diferentes, algo que puede indicar el desarrollo profesional con código compartido entre múltiples equipos.

Debido a los blancos elegidos, el uso de al menos una vulnerabilidad de día cero, la gran red de sitios web comprometidos y la naturaleza avanzada del malware utilizado, Symantec cree que Waterbug es un grupo patrocinado por un Estado (Symantec, 2016).

Phineas Fisher, alias @GammaGroupPR. El 3 de agosto de 2014 la cuenta parodia @GammaGroupPR publicó en Twitter un mensaje en el que anunciaba una filtración de los programas desarrollados por la empresa Gamma Internacional, especializada en el software espía FinFisher y cuyos clientes son gobiernos de todo el mundo. Un año después, el 6 de julio de 2015, Phineas Fisher ataca de nuevo contra otra empresa del sector, Hacking Team. La filtración de decenas de documentos internos de esta compañía italiana de seguridad informática, permitió saber, entre otras cosas, que España se encontraba entre sus clientes. En concreto, el CNI (y posiblemente también la Policía) habría contratado material de espionaje entre el que se incluía un sistema similar a un troyano y su mantenimiento, provocando protestas de organizaciones de defensa de los derechos civiles por considerar que el gobierno español carecía de cobertura legal para tales labores de rastreo. En abril de 2016, el hacker o los hackers bajo la identidad de Phineas Fisher publicaron el procedimiento por el que había llevado a cabo la intrusión contra Hacking Team. Una de sus últimas campañas ha sido el ataque a la cuenta de Twitter y a la web del sindicato de los Mossos d'Esquadra (policía autonómica de Cataluña), publicando decenas de datos personales de los agentes. Esta operación abrió de nuevo las dudas sobre la identidad de este grupo de atacantes (todo apunta a que se trata de un equipo) y su nacionalidad, pues los comunicados emitidos atribuyéndose esta acción parecen indicar un correcto dominio del castellano y el catalán, aunque el/los interesados lo negaron.

Delincuentes y mercenarios ocasionales

La ciberdelincuencia quedaría, teóricamente, fuera del ámbito de la ciberguerra: su objetivo es meramente económico y no se persigue ningún fin político o militar. Sin embargo, la alta capacidad técnica que cabe atribuir en general a quienes desarrollan estas acciones les convierte en un peligro en potencia, pues son susceptibles de realizar "servicios por encargo".

Desde el punto de vista de la ciberseguridad, después de la amenaza de las acciones de los distintos países, la ciberdelincuencia ocuparía el segundo lugar de preocupación como amenaza, según los servicios de inteligencia españoles: "El ciberdelito, su profesionalización y el crecimiento de la organización interna de sus actores han acaparado en 2015 el siguiente nivel de atención [tras los Estados]. La sofisticación de las técnicas usadas, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios delincuenciales bajo demanda) y la pulcritud en la perpetración de tales acciones constituyen una preocupación en franco crecimiento", asegura el CNI (Centro Criptológico Nacional, 2016).

Ciberdelincuencia rusa. La ciberdelincuencia rusa ocuparía, en este terreno, un lugar destacado con "múltiples operadores independientes que se dedican al delito informático sin relación con el Estado" (Goncharov, 2012). Operaciones de ciberespionaje relacionadas con el uso de malware espía de gran sofisticación como Octubre Rojo también parecen tener detrás a la delincuencia rusa.

Un estudio de noviembre de 2015, elaborado por la empresa de seguridad informática Kaspersky (2015), pormenoriza las actividades de estos grupos, su estructura, el precio de sus "productos" y "servicios" e, incluso, las ofertas de trabajo que generan. El impacto económico de sus acciones puede ser muy elevado. Por ejemplo, el grupo Carbanak[28] ("el mayor ladrón de bancos") habría causado pérdidas financieras que superarían los mil millones de dólares. Sin embargo, resulta aún más peligrosa la amplia gama de ataques que estos ciberdelincuentes ponen en el mercado. Según Kaspersky, entre los "productos" que desarrollan puede encontrarse software diseñado para obtener acceso no autorizado a un ordenador o un dispositivo móvil, con el fin de

obtener datos desde un dispositivo infectado o dinero de la cuenta de la víctima (los troyanos); software diseñado para aprovechar las vulnerabilidades en el software instalado en el ordenador de la víctima (exploits); ficheros con datos de tarjetas de crédito robadas y otra información valiosa; tráfico de Internet (aportar un cierto número de visitas a un sitio seleccionado por el cliente con usuarios de un perfil específico).

En cuanto a los "servicios" que prestan, abarcan una amplia gama: distribución de spam; organización de ataques DDoS (sobrecarga de sitios con solicitudes con el fin de evitar que estén disponibles para los usuarios legítimos); pruebas para la detección de malware antivirus; packing de malware (software malicioso "camuflado", para que no sea detectado por el software antivirus); alquiler de servidores; VPN (que proporciona el acceso anónimo a los recursos web, la protección del intercambio de datos); alquiler de alojamiento resistente (hosting que no responde a las quejas sobre el contenido malicioso y, por lo tanto, no se deshabilita el servidor); alquiler de botnets; evaluación de los datos de las tarjetas de crédito robadas; servicios para validar los datos (llamadas falsas, escaneo de documentos falsos); promoción de sitios maliciosos y publicidad en los resultados de búsqueda (black SEO); mediación en las transacciones para la adquisición de "productos" y "servicios"; retirada de dinero y cobro.

Los pagos de este tipo de "productos" y "servicios" en el mercado cibercriminal se hacen generalmente, según Kaspersky Lab, a través de un sistema de pago electrónico como WebMoney, Perfect Money, Bitcoin y otros.

Todos estos "productos" y "servicios" se compran y venden en varias combinaciones con el fin de permitir cuatro tipos principales de la delincuencia: ataques DDoS (ordenado o llevado a cabo con el propósito de extorsión); robo de información personal y datos de acceso a dinero electrónico; robo de dinero de las cuentas de los bancos u otras organizaciones; espionaje doméstico o corporativo; y bloqueo del acceso a datos en el ordenador infectado con el propósito de extorsión (ransomware) (Stoyanov, 2015).

Cibermercenarios árabes: The Desert Falcon. Los Halcones del Desierto (The Desert Falcon) son "un grupo de mercenarios que operan en

Oriente Medio y realizan operaciones de espionaje cibernético en la región. El grupo utiliza un arsenal de herramientas de malware de elaboración propia y técnicas para ejecutar y ocultar sus campañas en ordenadores y teléfonos móviles Android. Las primeras operaciones de los Halcones del Desierto se observaron en 2011 y sus primeras 'infecciones' son de 2013".

Los ataques van dirigidos a varias clases de víctimas, incluidas las organizaciones militares y gubernamentales, empleados responsables de las organizaciones de salud y lucha contra el blanqueo de dinero, instituciones económicas y financieras, destacados medios de comunicación, instituciones educativas y de investigación, empresas de energía y proveedores de servicios públicos, activistas y líderes políticos, empresas de seguridad física y otros objetivos con acceso a la información geopolítica importante. Utilizan una gran variedad de métodos y técnicas de ingeniería social para hacer llegar a las víctimas sus archivos y alentarlas a ejecutarlos.

Se estima que más de un millón de archivos fueron robados a sus víctimas, incluyendo comunicaciones diplomáticas de las embajadas, planes y documentos militares, documentos financieros, listas de contactos y archivos de medios de comunicación[29].

HACKTIVISTAS

Como fusión de los términos "hacker" (en su sentido original) y "activismo" surge hace casi dos décadas el concepto de "hacktivismo". De acuerdo a su definición original, recogida en HackStory[30], sería "hacer hacking, phreaking o crear tecnología para conseguir un objetivo político o social", según uno de los principales grupos que impulsaron esta práctica a finales de los años noventa, Cult of the Dead Cow. También es conocido como "desobediencia civil electrónica".

En el libro Ciberactivismo: las nuevas revoluciones de las multitudes conectadas (Tascón y Quintana, 2012), se aborda el

tema ampliamente. En resumen, el hacktivismo

consiste en la utilización de herramientas y medios digitales para la realización de acciones que llamen la atención de la sociedad, para así intentar conseguir cambios políticos o legislativos. Se basa en que quienes saben programar pueden alterar el correcto funcionamiento de las redes de comunicaciones o el propio Internet. Esas alteraciones llamarán la atención de la sociedad, que conocerá así los motivos de las protestas. Muchas veces, los hacktivistas son asociados a ciberterroristas, pero, al igual que en el mundo analógico, existen las mismas diferencias (y profundas) que entre activistas y terroristas, por más que las manipulaciones del lenguaje de los gobiernos que atacan los derechos humanos y las libertades civiles intenten unificar ambas etiquetas.

Otra importante novedad bien reciente es la democratización de las herramientas ciberactivistas. Si hace unos años uno tenía que ser un experto informático, o contar en el grupo u organización que encabezara la protesta con alguno, hoy cualquier persona, sin necesidad de conocimientos de programación, tiene a su alcance muchas de las herramientas que permiten realizar acciones llamativas. Lo que hasta hace bien poco estaba solo en manos de los ingenieros ha pasado a ser munición común del resto de la sociedad (Tascón y Quintana, 2012).

Entre las acciones llevadas a cabo por hacktivistas se encuentran las desfiguraciones de webs (cambiar el aspecto de un sitio web introduciendo lemas, fotos cómicas, etc.); los ataques de denegación de servicio (paralizar el sitio web atacado a costa del envío masivo de peticiones de páginas que consiguen que las máquinas que sirven las mismas no puedan hacerlo por saturación); mail bombing (envío masivo de correos a una dirección determinada que consigue llenar el buzón del destinatario y bloquearlo al no admitir más mensajes; software (desde herramientas de anonimato a programas para lanzar ataques contra otras organizaciones o portales de difusión de información, como WikiLeaks); webs espejo (clonar los contenidos de las webs que persiguen los gobiernos o las empresas para

complicar su cierre); Google bombing (técnicas de optimización para buscadores (SEO) para posicionar una página determinada entre los primeros resultados en Google cuando se busca una palabra); aplicaciones para boicots o el uso de redes sociales para la protesta social o la difusión de consignas (ibídem).

En sus inicios, se produjo una importante discusión en la comunidad hacker sobre la ética de estas acciones, en particular si suponían un ataque a la infraestructura de Internet, como los ataques de denegación de servicio[31].

Anonymous. La identidad difusa, heterogénea y distribuida que es Anonymous se encuadraría en este tipo de agentes. Anonymous no es un grupo hacker. De hecho, solo una pequeña parte de sus integrantes responderían al perfil clásico. Según la antropóloga Gabriella Coleman, "entre sus miembros, los geeks (fanáticos de las tecnologías, pero no necesariamente informáticos) serían los más numerosos. Aunque conviene tener un mínimo de conocimientos técnicos, no es imprescindible para ser un Anonymous. Cualquiera puede serlo". En su artículo publicado en El País, Elola (2011) describe lo que sigue:

He aquí la grandeza de Anonymous, solo hace falta un genio informático para programar la herramienta, y cuando esta herramienta pasa a ser usada por miles de personas anónimas, aunque no sean expertos a efectos prácticos, es como contar con un ciberejército de miles de hackers que pueden inutilizar cualquier red o sistema informático si se lo proponen.

Tal como contábamos en Cibertactivismo… (Tascón y Quintana, 2012), los orígenes de Anonymous se encuentran en 4chan.org, web creada en 2003 por Christopher Poole, entonces un adolescente neoyorkino de 15 años, como réplica del japonés 2chan. Los Anonymous de 4chan.org se asocian con acciones de gamberrismo digital tales como bromas telefónicas, divulgación de información privada en Internet o ataques de denegación de servicio (DDoS).

Sin embargo, en 2008, se produce un punto de inflexión en la dinámica del colectivo con el Proyecto Chanology, una operación contra el oscurantismo y los mensajes pseudocientíficos de la Iglesia de la Cienciología. La acción fue relevante, además de por estar orientada a un propósito, porque supuso la primera acción presencial del movimiento: el 10 de febrero de 2008, más de 6.000 personas protestaron en Norteamérica, Europa, Nueva Zelanda y Australia, muchos frente a las iglesias de la Cienciología. Fue entonces cuando se escenificó la que sería la imagen del movimiento: individuos con la máscara de Guy Fawkes como reivindicación no tanto del anonimato como de la idea de que "cualquiera es Anonymous". En algunos de sus escritos se hace uso de la frase "We the people", "nosotros, el pueblo", que sustenta el lema del movimiento: "Somos legión" (ibídem).

Ciberguerra contra el hacktivismo. En ocasiones, el hacktivismo puede suponer una importante herramienta de oposición al poder político de los países, como en Turquía, México, Venezuela o en la denominada Primavera Árabe. En algunos casos, ante esta situación, los gobiernos ponen en marcha auténticas iniciativas de "ciberguerra" contra los activistas.

En México está documentado el uso de botnets (redes de ordenadores zombies) por el entorno del presidente Enrique Peña Nieto contra movimientos y grupos sociales para neutralizar las protestas (e incluso, supuestamente, alterar resultados electorales) (Escorcia, 2013; Finley, 2015; Robertson, Riley y Willis, 2016).

En Túnez, durante las revueltas de 2011, el Gobierno llevó a cabo una extensa ofensiva online: desde ataques por phishing para robar contraseñas de activistas y poder espiarles, a hacer caer webs o bloquear cuentas en redes sociales (Ryan, 2011).

CIBERVÁNDALOS

Con frecuencia, los medios de comunicación sitúan las acciones de cibervándalos y script kiddies en el ámbito de la ciberguerra (al

entrar su actividad dentro de la categoría genérica de “ataques informáticos”). Sin embargo, sus ataques, de poca envergadura en general, no tendrían ninguna finalidad política, económica o activista, más allá de llevarlos a cabo “porque se puede”.

Un informe del CNN denomina “cibervándalos” a “aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo” (Centro Criptológico Nacional, 2016). Comparten la falta de motivación con los llamados script kiddies, pero estos tendrían, por el contrario, “conocimientos limitados y harían uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío” (ibídem). Algunos ciberataques del entorno yihadista antes mencionados se podrían encuadrar en esta esfera.

En ocasiones, las acciones que llevan a cabo obtienen una amplia atención mediática por lo llamativo de sus objetivos, pero, según los servicios de inteligencia, “no constituyen una amenaza seria a los intereses de las organizaciones”. Un ejemplo de este tipo de agente sería el grupo autodenominado “Lizard Squad” (Escuadrón Lagarto), responsable en 2015 del ataque a la web de Malaysia Airlines.

Lizard Squad es un grupo conocido por atacar a grandes empresas como Sony y Microsoft. Su símbolo es un lagarto que fuma en pipa, con frecuencia con sombrero de copa. Se dieron a conocer en agosto de 2014 al atacar a la plataforma de juegos online de PlayStation de Sony. Antes, habían atacado otros sitios de juegos como Runescape, World of Warcraft y League of Legends, cuyos servidores dejaron fuera de línea con un ataque DDoS (su forma de ataque habitual), lo que fue considerado como la primera acción del grupo. En diciembre de 2014, atacaron de nuevo la red de PlayStation y también la de Xbox. Por esas mismas fechas, Corea del Norte vivió un apagón de Internet, que el grupo se atribuyó. Fue un ataque distribuido de negación de servicio por el que el país quedó desconectado durante 24 horas. Cuatro días después, el grupo ejecutó el que quizá ha sido su intento más ambicioso: atacar la red Tor, aunque con escaso éxito. Esta iniciativa ocasionó la respuesta de Anonymous, quienes, además, habrían llevado a cabo acciones contra alguno de sus miembros (captura y publicación de sus datos

personales) (Alonso, 2014).

Lizard Squad también afectó al sitio web de Malaysia Airlines, redireccionando a sus usuarios a una página completamente diferente, con el logo del grupo. Durante este ataque, los hackers publicaron un mensaje que afirmaba que la página había sido tomada por el Cibercalifato, en alusión a sus vínculos con el grupo extremista Estado Islámico, al que suele mencionar con frecuencia a través de su cuenta de Twitter[32]. También han realizado ataques contra redes sociales como Facebook e Instagram. A principios de 2005, dos de sus miembros (se cree que estaría formado por entre 7 y 15) fueron arrestados por la policía (Alonso, 2015).

EMPRESAS

El ciberespionaje industrial, a juicio de los servicios de inteligencia, es otro de los escenarios que hay que tener en cuenta. “En el caso del ciberespionaje industrial, son las organizaciones privadas las que actúan de atacantes (en ocasiones también los Estados). El lucro derivado de una obtención ilícita de información y el deterioro intencionado de los sistemas de la competencia son buenos motivos para que las organizaciones del sector privado desarrollen ciberataques”, advierte el CNN (Centro Criptológico Nacional, 2016).

Capítulo 3

ASÍ SE LUCHA EN LA CIBERGUERRA: de los ataques DDoS al secuestro de sistemas

Año 2011. Los virus keylogger son viejos conocidos de los atacantes informáticos. Se utilizan sobre todo para capturar contraseñas, datos de tarjetas de crédito y números de cuentas bancarias cuando los usuarios los escriben en sus teclados. Los datos se envían a continuación a los defraudadores a través de Internet. En octubre de 2011, uno de estos programas malignos había infectado nada menos que los sistemas que controlaban los aviones no tripulados (drones) que la Fuerza Aérea norteamericana tenía desplegados en frentes de guerra, según una exclusiva de la revista Wired (Shachtman, 2011).

Verano de 2015. El Instituto Nacional de Ciberseguridad español se hace eco de esta escalofriante noticia (INCIBE, 2015a; Gaffey, 2015): según la revista Behörden Spiegel, seis lanzaderas de misiles y dos radares Patriot alemanes, desplegados en Turquía cerca de la frontera con Siria, habrían ejecutado órdenes desconocidas durante un periodo de tiempo limitado. Como era de esperar, el Gobierno alemán niega la información. Supuestamente, estos comandos habían sido transmitidos por una "fuente extranjera desconocida".

En diciembre de ese mismo año, la red eléctrica nacional de ucrania sufre un ataque informático que provoca un corte de suministro durante varias horas. 600.000 hogares de la región de Ivano-Frankivsk se quedan sin electricidad. El ataque se habría realizado mediante el uso del troyano BlackEnergy y de técnicas de ingeniería social. Fue la primera vez en la historia que un ataque informático era capaz de provocar un corte de suministro eléctrico (INCIBE, 2015b). El ataque se atribuyó a Rusia, aunque, una vez más, se puso en evidencia la dificultad para determinar con precisión la autoría final de un ciberataque (Fojón, 2016).

Estos episodios, entre otros tantos, muestran cómo las armas que se emplean en los combates y escaramuzas de la ciberguerra, y también los objetivos a batir, han cambiado. A continuación se resumen las ofensivas y formas de ataque más relevantes en este nuevo escenario. Un aspecto importante de esta relación es la muy

diversa gravedad que representan y merece la pena que nos detengamos a observar. Las noticias que nos llegan de estas acciones a través de los medios de comunicación suelen ser bajo la categoría genérica de “ataque”, independientemente de su naturaleza y del daño real provocado. Esto puede favorecer una percepción distorsionada de las mismas, lo que en ocasiones se busca de forma interesada.

Por ejemplo, cuando la Policía española difundió la detención de lo que llamó “cúpula de Anonymous”, para contextualizar (según sus intereses, cabe entender) el alcance de la operación, recordó, desde su muy seguida cuenta de Twitter, que los activistas habían “atacado a” la Junta Electoral. En realidad, lo que ocurrió fue una acción de “desfiguración” de la web (una modificación temporal de su aspecto para incorporar una consigna) efímera y sin daños cuantificables o irreversibles.

ATAQUES DE 'DÍA CERO'

"Día cero" puede hacer referencia a dos conceptos: una vulnerabilidad de día cero o un exploit de día cero (Zetter, 2014b). La vulnerabilidad de día cero es un fallo de seguridad en el software (como el software del navegador o del sistema operativo), aún desconocido para el fabricante de software o de los proveedores de antivirus. Por ello, no hay parches disponibles aún y, en general, los antivirus no pueden detectar el malware que se aprovecha de este fallo. Un exploit de día cero es el código que los atacantes utilizan para aprovechar una vulnerabilidad de día cero e infectar el equipo con un virus, troyano u otro software malicioso sin ser detectado.

El concepto "día cero" alude al número de días que el proveedor del software tiene conocimiento del fallo antes de que sea explotado por algún atacante (ningún día, puesto que no es consciente de él). Las vulnerabilidades y exploits de día cero son muy valiosos y buscados tanto por cibercriminales como por agencias de inteligencia gubernamentales. Son poco frecuentes y en el mercado negro pueden alcanzar un valor muy elevado, aunque su precio varía en función, entre otros factores, de la dificultad que permiten sortear. Algunos de los más famosos ataques que han utilizado ataques de día cero han sido:

Stuxnet. Virus o gusano dirigido contra el programa nuclear iraní. Utilizó cinco ataques de día cero para propagarse y obtener acceso privilegiado en los sistemas.

Operación Aurora. El ataque de hackers chinos en 2010 contra Google, Adobe y más de una docena de otras empresas. Utilizó una vulnerabilidad de día cero que se encuentra en varias versiones del software del navegador Internet Explorer de Microsoft.

RSA. Los atacantes de la empresa de seguridad digital RSA

utilizaron un exploit de día cero en el reproductor Flash de Adobe en un ataque de phishing contra los empleados de esta compañía.

SOFTWARE MALICIOSO (MALWARE)

Son programas específicamente creados para realizar un ataque. Se emplean para fines variados: desde el cibercrimen al espionaje online o la ciberguerra. Existen distintos tipos de malware según la "misión" para la que hayan sido creados[33]:

Virus clásicos. Programas que infectan a otros programas para tomar después el control de ejecución de los archivos infectados. La velocidad de propagación de los virus es algo menor que la de los gusanos.

Gusanos de red. Este tipo de malware usa los recursos de red para distribuirse. Su nombre implica que pueden penetrar de un equipo a otro como un gusano. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.

Troyanos. Esta clase de malware (denominados también "caballos de Troya") incluye una gran variedad de programas que efectúan acciones sin que el usuario se dé cuenta y sin su consentimiento: recolectan datos y los envían a los criminales; destruyen o alteran datos con intenciones delictivas, causan desperfectos en el funcionamiento del ordenador o usan los recursos del ordenador para fines criminales, como hacer envíos masivos de correo no solicitado. No son virus clásicos porque no infectan otros programas o datos. Los troyanos no pueden penetrar en los equipos por sí mismos, sino que se propagan bajo la cobertura de algún software "deseable". Son capaces de causar mucho más daño que los virus clásicos.

Spyware. Es un software que permite recolectar información sobre un usuario u organización de forma no autorizada. Su presencia puede ser completamente invisible para el usuario. Pueden recoger datos sobre las acciones del usuario, el contenido del disco duro, el software que tiene

instalado, la calidad y velocidad de la conexión, etc. Pero no es su única función. Son conocidos por lo menos dos programas (Gator y eZula) que permiten también controlar el equipo. Otro ejemplo de programas espías son los que instalan su código en el navegador de Internet para redireccionar el tráfico a una web que no hemos solicitado.

Phishing. Es una variedad de programas espías que se propaga a través del correo con el objetivo de obtener datos confidenciales del usuario, de carácter bancario preferentemente. Los correos de phishing están diseñados para tener el mismo aspecto que los que el usuario esperaría recibir de instituciones o marcas conocidas. Los correos contienen un enlace que redirecciona al usuario a una página falsa que solicita que se introduzcan datos confidenciales, como el número de la tarjeta de crédito.

Riskware. No son programas maliciosos, pero contienen una amenaza potencial. En ciertas situaciones ponen sus datos en peligro. Incluyen programas de administración remota, marcadores, etc.

Joke. Es un tipo de virus informático cuyo objetivo es crear algún efecto molesto o humorístico (como una broma). Es el tipo de malware que menos daño produce en el ordenador.

Rootkits. Un rootkit es una colección de programas usados por un atacante para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador. Esto se logra de dos formas: reemplazando archivos o bibliotecas del sistema o instalando un módulo de kernel. El cracker instala el rootkit después, obteniendo un acceso similar al del usuario: por lo general, craqueando una contraseña o explotando una vulnerabilidad, lo que permite usar otras credenciales hasta conseguir el acceso de raíz o administrador.

Otros programas maliciosos. Son una serie de programas que no afectan directamente a los ordenadores, pero que se usan para crear virus, troyanos o para realizar actividades ilegales como ataques DDoS y penetrar en otros ordenadores, etc.

Spam. Se trata de mensajes no solicitados de remitente desconocido enviados en cantidades masivas de carácter publicitario, político, de propaganda, solicitando ayuda, etc. Otra clase de spam tiene como objetivo hacer propuestas relacionadas con operaciones ilegales que

involucran dinero o participación en algún "supernegocio". También hay correos dedicados al robo de contraseñas o números de tarjetas de crédito, cartas de cadena, etc. El spam genera una carga adicional a los servidores de correo y puede causar pérdidas de la información deseada.

SECUESTRO DE SISTEMAS: RANSOMWARE

El ransomware es un tipo de malware que funciona como mecanismo digital para la extorsión: bloquea el acceso a un sistema informático hasta que el usuario o compañía paga un rescate. En principio, este tipo de acción entraría más en el ámbito de la ciberdelincuencia que de la ciberguerra propiamente dicha. Aunque no se puede descartar que pueda llegar a ser usado (o que se esté usando ya) como vía de obtener financiación para otro tipo de ofensivas (Kaspersky Lab, 2015).

Sus primeros casos se dieron entre 2005 y 2009 en Rusia y los países de Europa del Este. Hoy, supone una amenaza emergente que presenta un crecimiento exponencial: solo en el ámbito empresarial, Kaspersky detectó, en el año 2015, 50.000 equipos afectados, el doble que el año anterior. Symantec ha estimado que cada año los ciberdelincuentes obtienen al menos cinco millones de dólares con este tipo de extorsiones. Los programas más extendidos a través de los que se realizan estos ataques son CryptoWall, CTB-Locker, and TorrentLocker.

Normalmente, un ataque de ransomware se lleva a cabo a través de un correo electrónico que incluye un archivo o una imagen adjunta que puede ser ejecutable. Una vez que se abre el archivo adjunto, el malware invade el sistema del usuario. Un ransomware también podría acceder a un ordenador visitando un sitio web con malware. Una vez en la página web, el usuario, sin saberlo, ejecuta un script inseguro (a veces al hacer click en un link o al descargar un archivo) y es entonces cuando el malware invade el sistema.

Cuando el equipo de un usuario se infecta, nada visible sucede de inmediato. El malware opera silenciosamente en un segundo plano hasta que el sistema o el mecanismo de bloqueo de datos se activa y se compromete. Los cibercriminales son cada vez más hábiles en el desarrollo de ransomware y tienen muchas herramientas y técnicas a su disposición para asegurarse de que no sea descubierto por la

víctima. Luego aparece un cuadro de diálogo que notifica al usuario el bloqueo de los datos y exige el pago de un rescate para recuperar el acceso. En ocasiones, si el ataque va dirigido contra empresas, también se pide como rescate información comercial sensible (propiedad intelectual). Aunque lo frecuente es que se dirija contra ordenadores, existe una tendencia creciente de ataques de ransomware contra dispositivos móviles. Casos recientes han sido el de tres centros médicos norteamericanos en el espacio de un mes (marzo-abril de 2016), que parecen ser un blanco propicio para este tipo de ataques (Zetter, 2016c). En España, a finales de abril de 2016, varios departamentos el Ministerio del Interior fueron víctimas de un ataque de este tipo (Ballesteros, 2016).

EL INTERNET DE LAS COSAS Y CIBERGUERRA

El Internet de las Cosas (en inglés, Internet of Things) es el escenario tecnológico al que nos dirigimos. Básicamente, se trata de conectar cualquier dispositivo a Internet y los dispositivos entre sí. Esto incluye todo: teléfonos móviles, cafeteras, lavadoras, auriculares, lámparas, televisiones, ordenadores portátiles y casi cualquier cosa que se pueda imaginar, como automóviles o cualquier otro medio de transporte, sensores de todo tipo o las prestaciones de domótica de nuestros hogares. Esto también se aplica a los componentes industriales, a las instalaciones urbanas y a cualquier infraestructura.

Para Morgan (2014), "El Internet de las Cosas es una red gigante de 'cosas' conectadas (que también incluye a las personas). La relación será entre la gente y la gente; entre la gente y las cosas, y entre las cosas-cosas. La nueva norma para el futuro va a ser: 'Cualquier cosa que se puede conectar, estará conectada'". Esta nueva realidad plantea numerosos retos desde el punto de la vista de la seguridad. En España, el Centro Criptográfico Nacional (2016) lo advierte en su informe sobre vulnerabilidades emergentes: "El incremento del denominado Internet de las Cosas y de sus usuarios seguirá atrayendo el interés de los ciberdelincuentes. No solo de los dispositivos (teléfonos, tabletas, TV, wearables [dispositivos que se llevan siempre encima y que siempre están encendidos], luces, coches, electrodomésticos) de los que se puede extraer una cantidad ingente de información, sino también de los servicios que están detrás conectados a una central en la nube".

El Internet de las Cosas se puede convertir en blanco de amenazas que ya se daban pero que ahora adquieren una dimensión universal:

Hackeo o manipulación de dispositivos

Al igual que ocurre en los ataques contra infraestructuras críticas, en los que una manipulación del software que los controla puede provocar el mal funcionamiento de los equipos o instalaciones, e incluso su deterioro o destrucción, cualquier dispositivo conectado a Internet es ahora susceptible de ser atacado. Teniendo en cuenta que los objetos conectados en este Internet de las Cosas incluyen desde un vehículo sin conductor a dispositivos médicos, podemos aventurar los posibles escenarios catastróficos que podrían darse. La manipulación de los dispositivos puede buscar no solo causar desperfectos en los mismos, sino modificarlos con fines maliciosos.

Recientemente, la periodista especializada Kim Zetter (2016c) advertía en Wired:

Algunos tipos de manipulación de datos podrían incluso dar lugar a muertes. En 1991, un misil Patriot en Arabia Saudita durante la primera guerra del Golfo no logró interceptar un misil Scud entrante debido a un fallo de software en el ordenador de control del arma, permitiendo que el Scud golpeara un cuartel del ejército y matase a 28 soldados. De nuevo, esto fue un error involuntario. Pero los espías chinos han invadido numerosas redes de contratistas del Departamento de Defensa de Estados Unidos en la última década, lo que aumenta la preocupación entre los funcionarios militares de que no solo están robando planos para copiar las armas, sino que también pueden alterar o insertar código para sabotear la integridad de los sistemas de armas y cambiar la forma que operan.

El secuestro de los dispositivos con técnicas análogas al ransomware es otro riesgo posible.

Ciberespionaje

Edward Snowden, el exanalista de la NSA que filtró cómo la agencia de espionaje norteamericana nos espía de forma masiva, bromeaba sobre la ralentización de la implantación del Internet de las Cosas, a raíz de un estudio que desvelaba el escaso interés de los usuarios por adoptar este tipo de tecnología en su vida cotidiana. “No me explicó por qué”, remachaba con sorna. Las filtraciones de Snowden han supuesto no solo una mayor preocupación por la privacidad y seguridad de nuestras actividades digitales más cotidianas (chatear, enviar correos o navegar por Internet), sino también la adopción de una cierta autocensura. No hace mucho, una encuesta de Pew Research reflejaba qué no hacer respecto a dispositivos como los wearables, que reportan de forma continua, incluso nuestras constantes vitales.

En el escenario de cibervigilancia global que los papeles desvelados por Snowden muestran, el Internet de las Cosas, donde cualquier dispositivo es un recolector de información, nuestra intimidad aún será más precaria.

El ascenso de las redes de zombis del Internet de las Cosas

Igual que ya es habitual que en muchos de los ataques informáticos que se llevan a cabo se utilice una red de ordenadores controlados de forma remota sin que su dueño legítimo sea consciente de ello (lo que se conoce como “botnet”), “una tendencia que ya hemos descubierto es el requisado de los dispositivos IO [del Internet de las Cosas] en favor de las redes de bots”, advertía en Wired la periodista especializada Kim Zetter:

En lugar de los piratas que secuestran su ordenador portátil para su ejército de zombies, ahora van a comandar grandes redes de dispositivos IO como las cámaras de vigilancia de circuito cerrado

(CCTV), televisores inteligentes y sistemas de automatización del hogar. Ya hemos visto cómo las cámaras de CCTV se convirtieron en ejércitos botnet para lanzar ataques DDoS contra bancos y otros objetivos. A diferencia de un ordenador de sobremesa o portátil, puede ser más difícil saber cuándo el tostador conectado se ha enrolado en un ejército bot.

ATAQUES A INFRAESTRUCTURAS CRÍTICAS

Los ataques a infraestructuras críticas se encuentran entre los ataques más difíciles de ejecutar, pero también entre los más peligrosos. El objetivo es el daño físico a sistemas, máquinas, edificios o instalaciones relacionadas con la prestación de servicios esenciales como el sector energético, la canalización de aguas, los servicios de telefonía o cualquier proceso industrial. Sin embargo, no hay una definición universal de "infraestructura crítica", y Estados Unidos, por ejemplo, incluye a su industria cultural en esta categoría (Zetter, 2016a). Interrupciones del suministro eléctrico, ataques a las redes de telefonía o al sistema de una presa son casos recientes de este tipo de ofensiva que puede tener un alcance incalculable.

La aseguradora norteamericana Lloyd's estimaba que el daño de un posible ciberataque contra la red de energía eléctrica solo del noreste de Estados Unidos tendría un coste por encima de un billón (trillion) de dólares (Camhi, 2016).

Las estadísticas que dan cuenta de estos posibles incidentes no son muy fiables, pues engloban todo tipo de ataques relacionados con las empresas prestadoras de estos servicios, aunque el impacto en el funcionamiento de sus instalaciones sea bajo o nulo (como spam, phishing contra otros usuarios utilizando su identidad corporativa, intrusiones en la red de ofimática, o que se "caiga" su web por un DDoS) (Martínez, 2015). Es decir, sucesos con un daño a la gestión de la compañía o a su reputación más que a la infraestructura en sí misma.

El caso del virus Stuxnet que se narra en detalle en el capítulo siguiente entraría en este grupo de ataques.

Otros episodios de incidentes contra infraestructuras críticas han sido: el ataque a un sistema de canalización de agua en Springfield (Estados Unidos) en 2011 (Zetter, 2011a); la "destrucción" o

inutilización de 35.000 ordenadores de la red de la petrolera Saudí Aramco —en lo que se calificó “el hackeo más grande de la historia” (Pagllery, 2015)—, provocando interrupciones en la distribución del crudo en 2012; o el corte de suministro eléctrico de toda una región de Ucrania en diciembre de 2015[34].

El caso de la presa de Nueva York y cómo lo hackers utilizaron Google para piratearla

Entre al menos aproximadamente el 28 de agosto de 2013 y, por lo menos, alrededor del 18 de septiembre de 2013, Hamid Firoozi, el acusado, obtuvo en repetidas ocasiones acceso remoto no autorizado a un ordenador que controla el sistema de control y supervisión (SCADA) de la presa de Bowman, una presa situada en Rye, Nueva York. El acceso al sistema SCADA de la presa de Bowman permitió a Firoozi obtener repetidamente información sobre la situación y el funcionamiento de la misma, lo que incluye, entre otras cosas, información sobre los niveles de agua y la temperatura, y el estado de la compuerta que se encarga del control de los niveles de agua y caudales. Aunque el acceso al sistema SCADA normalmente también habría permitido a Firoozi operar y manipular la compuerta de la presa de Bowman de forma remota, el control de la compuerta había sido desconectado manualmente por problemas de mantenimiento antes del momento en que Firoozi tuvo acceso a los sistemas[35].

La anterior cita es un fragmento de la acusación de un juzgado federal norteamericano contra siete piratas informáticos iraníes de marzo de 2016 (Cox, 2016). La fiscal les atribuye los ataques de denegación de servicio (DDoS) contra numerosas compañías financieras, como el Banco de América o JP Morgan y, además, una intrusión en el sistema de control de una presa, que, aunque ocurrió en 2013, no se informó hasta diciembre de 2015 (Yadron, 2015).

La “presa” de la avenida Bowman, en la pequeña localidad de Rye Brook (Westchester, Nueva York), es en realidad una compuerta para controlar las crecidas de un pequeño arroyo o torrentera. Construida en 1900, se encuentra actualmente entre una maraña de maleza y rocas y está prácticamente en desuso. El alcalde, sorprendido de que su pueblo (8.000 habitantes) fuese objetivo de los piratas informáticos iraníes, especuló con la posibilidad de que se hubiesen equivocado de presa (por una llamada Arthur R. Bowman, del Estado de Oregón, de dimensiones mucho mayores: 77 metros de altura por 244 metros de ancho) o que estuviesen ensayando para un ataque mayor (Berger, 2016).

Más tarde se supo que los hackers (crackers) habrían empleado, para seleccionar este objetivo, una técnica de búsqueda en Google que sirve para identificar sistemas vulnerables denominada “Google dorking” (Matthews, 2016; Bort, 2016). Se trata de un proceso que puede utilizar desde un pirata informático a un empleado de seguridad con el fin de, con ciertos parámetros de búsqueda, localizar sistemas informáticos desprotegidos. Firoozi, supuestamente, había estado utilizando esta técnica de Google durante meses en busca de sistemas de control industrial vulnerables en Estados Unidos, como un ordenador que utilizase un viejo sistema operativo o que no hubiera sido actualizado con un parche de seguridad.

INGENIERÍA SOCIAL

La ingeniería social no es un ataque aislado, sino más bien un conjunto de técnicas que se ponen en práctica para poder llevar a cabo, en alguna de sus fases, algunos de los ataques aquí descritos. Por ejemplo, el “USB tirado en el suelo” que se menciona en el caso de Agent.btz sería uno de estos métodos que se basan en el “fallo humano” para lograr un propósito, como infectar un equipo no conectado a Internet.

Los ataques por phishing (mensajes que parecen auténticos pero que no lo son) también utilizan la ingeniería social para poder tener éxito. El principio que sustenta la ingeniería social es que, en cualquier sistema, “los usuarios son el eslabón débil”. En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser quien no es y de este modo lograr información sensible (una contraseña) o que se realice una determinada acción (pinchar un enlace, abrir un archivo o conectar un dispositivo extraíble no seguro).

ATAQUES DDoS

Las siglas DoS corresponden a “deny of service” o “denegación de servicio”. Se refieren a un ataque mediante una avalancha de peticiones simultáneas enviadas a un sitio web para ver sus páginas, haciendo que el servidor web se bloquee o, simplemente, deje de funcionar en su intento de responder a más solicitudes de las que puede manejar. Hay otros tipos de ataques de denegación de servicio que utilizan diferentes tácticas, pero todos tienen el mismo efecto: impedir el acceso a un sitio web.

DDoS hace referencia a un ataque distribuido de denegación de servicio, es decir, que el ataque proviene de múltiples máquinas distribuidas en varios lugares en Internet. Ahora son los más frecuentes, en lugar de los DoS, realizados desde una sola máquina.

Los DDoS se llevan a cabo mediante una botnet o red de ordenadores zombies controlados por los asaltantes de forma remota. De este modo, los equipos se usan como un ejército que se dirige contra un sitio web o sistema comprometido. El equipo de cualquier usuario puede convertirse en “zombi” si es infectado con un software malicioso con este propósito. Una botnet también se puede utilizar para propagar virus, generar spam y cometer otros tipos de delitos y fraudes en Internet.

Aunque no es fácil parar el ataque o identificar su procedencia, y la solución con frecuencia es “dejar que pase”, las entidades o empresas con más recursos para invertir en servidores tienen más posibilidad de hacer frente a un ataque de este tipo: “Los DDoS son realmente algo concreto, un golpe fuerte y certero, pero no algo continuado en el tiempo. Por ello, solo son efectivos si consiguen dejar sin servicio la página antes de que sus administradores puedan tomar medidas, como redirigir el tráfico a otros servidores”, según explican en TicBeat[36].

Los ataques DDoS no se limitan a los ordenadores y servidores web,

sino que pueden dirigirse a los sistemas telefónicos. Es importante observar que el daño real que provocan estos ataques es, en general, muy limitado, y no va más allá de la interrupción temporal del acceso a una web, con lo que puede suponer de molestia (o pérdida de negocio, por ejemplo, en el caso de una web de comercio online). Pero muy lejos de las versiones catastrofistas con que se suelen presentar:

A pesar de que la potencia de los ataques DDoS está creciendo, los medios de comunicación a menudo los caracterizan de forma errónea y exageran su importancia. Muchas agencias de noticias, por ejemplo, se han referido erróneamente a los ataques contra los sitios web de Estonia en 2007 como “la guerra cibernética” (entre ellos, un artículo de la revista Wired). Y, en una historia de 2012 de Bloomberg, que describe los ataques DDoS contra los bancos de Estados Unidos, la cadena de noticias escribió que los ataques habían “violado algunas de las defensas informáticas más avanzadas de la nación” y que el rango de este tipo de ataques “se encontraba entre los peores escenarios previstos por la Agencia de Seguridad Nacional” (Zetter, 2016a).

ATAQUES DE ‘BAJA INTENSIDAD’: DESFIGURACIÓN DE WEBS

En el apartado de ataques de “baja intensidad”, por lo efímero de los daños que normalmente provocan, podemos situar las desfiguraciones de webs, que consisten en alterar temporalmente el aspecto de una web introduciendo algún lema, mensaje o imágenes. Se puede entender que cumplen la misma función que un grafiti o una pintada en un muro (en este caso, digital), pero con una capacidad de comunicación directa de la acción muy superior. Su impacto no reside tanto en los daños que causan (escasos y temporales) como en lo llamativo de la acción y el efecto multiplicador que suele conseguir: “Cualquiera puede acercarse virtualmente a la web desfigurada para ver la intervención, con lo que el efecto se multiplica porque no necesita de muchos intermediarios clásicos (los medios) para darse a conocer. Las acciones de sabotaje similares en el mundo analógico solo podían ser conocidas por los que se encontraban cerca o, alguna vez, con suerte, por la transmisión de los medios de comunicación” (Tascón y Quintana, 2012).

También provocan un daño real limitado, reducido en general a la visibilidad de la acción cuando se comprometen perfiles en redes sociales. La suplantación suele ser evidente y por un tiempo muy reducido antes de que su dueño legítimo vuelva a tomar el control de su cuenta.

Nuevas tácticas: de la geometría al Big Data

Antes, en las guerras, lo importante era la geometría: fortificaciones, defensas, organización de ataques… Poco a poco, se fue haciendo más necesario el cálculo y, hoy en día, hay un gran territorio para la estadística, como en el análisis de modelos, especialmente si tienen que ver con la predicción del comportamiento enemigo.

Para comprender cómo empezó todo, nos tenemos que remontar a principios del siglo pasado. En la primera guerra mundial, un extraño personaje británico del servicio de ambulancias que acompaña a la decimosexta división de infantería francesa aprovecha los momentos de inactividad en el frente para hacer cálculos y experimentos. Trabaja sobre una bala de heno que le sirve de pupitre. Los soldados le llaman "El profesor". Hablamos de Lewis Fry Richardson, matemático, físico y pacifista. Antes de la guerra ejercía como director del laboratorio de investigación de la Oficina Meteorológica de Gran Bretaña (un puesto que abandonará más tarde, por razones de objeción de conciencia, cuando este organismo quede adscrito a la Real Fuerza Aérea británica).

Richardson, como otros científicos, fue un adelantado a su tiempo. Sin que aún estuviera disponible la tecnología para ponerlo en práctica, diseñó sistemas de predicción meteorológica basados en modelos matemáticos y cálculos estadísticos. Sus trabajos son el fundamento de los métodos actuales de predicción del tiempo y se basan en el análisis de gran cantidad de datos, que ahora sí se pueden llevar a cabo gracias los ordenadores capaces de efectuar en poco tiempo las operaciones necesarias.

La guerra, igual que la atmósfera, pensaba Richardson, "lejos de ser un accidente imprevisible, podría ser la consecuencia de leyes aún desconocidas que funcionarían a partir de hechos medibles. Debajo de su curso, aparentemente aleatorio y caótico, estarían los patrones regulares de estas leyes. Con los datos correctos y las ecuaciones

correctas, la guerra podría ser predecible y, por lo tanto, se podría prevenir" (Berreby, 2014).

Richardson estaba buscando una manera de pronosticar la guerra al igual que se podía pronosticar el tiempo. Su objetivo era encontrar cantidades medibles y leyes inexorables que pudieran ser modeladas con ecuaciones. Durante dos décadas antes de su muerte, en 1953, Richardson recogió cuidadosamente datos sobre la carrera de armamentos, variaciones en los indicadores económicos, insurgencias, revoluciones, disturbios y combates. A continuación, ordenó los conflictos según su gravedad (en función del número de muertes), de modo análogo al modo en que los geólogos clasifican los terremotos. Y encontró algo interesante:

Al igual que la atmósfera está llena de pequeños remolinos, la humanidad experimenta muchas pequeñas disputas mortales, que se traducen en unas pocas muertes. Pero de vez en cuando vienen enormes tormentas, que matan a millones de personas. Estos son precisamente el tipo de brotes —igual que la guerra mundial que Richardson había visto por sí mismo— que la gente considera sorprendentes. Sin embargo, cuando representó la frecuencia de las guerras en función del número de muertes causadas por cada uno de ellas, encontró una relación constante y predecible. En sus gráficos, la violencia obedecía a una "ley potencial" —una relación constante entre el tamaño y la frecuencia de los sucesos—. Al igual que los terremotos gigantes (que también obedecen a una "ley potencial"), las guerras gigantes no eran terribles sorpresas que surjan de circunstancias únicas. Parecían ser más o menos predecibles (ibídem).

Sus trabajos en este campo se recogen en su obra The Statistics of Deadly Quarrels, publicada póstumamente en 1960.

Décadas después, un grupo de investigadores exploraría la misma idea de Richardson: la posibilidad de pronosticar una guerra a partir del análisis de grandes cantidades de datos (Big Data).

Neil Johnson, un físico de la Universidad de Miami; Michael Spagat, economista de la University College de Londres, junto con otros científicos de datos, como Sean Gourley, encontraron en 2009 una "ley potencial" similar analizando cifras de guerras convencionales, ataques terroristas y ataques cibernéticos. Sus resultados, publicados en la revista Nature (Bohorquez et al., 2009), ofrecían algunas sugerencias sobre cuándo es más probable que ocurran futuros ataques o cómo se puede actuar de forma más efectiva para tratar de prevenirlos.

Su trabajo mostraba que la sincronización de los ataques, así como su gravedad, respondían a patrones predecibles. Además, observaron similitudes con los modelos del mercado financiero, dándose una sorprendente relación entre las formas violentas y no violentas de la conducta humana, según sus cálculos. Para llegar a estas conclusiones, los investigadores habían reunido datos sobre todo tipo de conflictos, incluyendo cibersabotajes, de 130 fuentes de información diferentes (Gourley, 2009)[37]: ONG, periódicos o canales informativos de televisión, como CNN o Al Jazeera. Tras filtrarlos, construyeron una base de datos con categorías como "localización", "país", "número de muertos", "número de heridos", "fecha" o "tipo de arma". Analizando los datos, vieron que obedecían a una distribución de probabilidad típica que podía expresarse mediante una ecuación matemática. Habían dado con la fórmula que servía para pronosticar una guerra: $P(x) = C(x)-\alpha$.

Las posibilidades que ofrecen las técnicas de Big Data para anticiparse a los conflictos nos permiten exigir una nueva forma de gestión de los mismos a los gobiernos y organismos encargados de ello. Por ejemplo, a raíz de la crisis de los refugiados, una tribuna de opinión en la revista americana Wired argumentaba que los datos permitían haber previsto la tragedia que se avecinaba y criticaba que no hubiese ocurrido así para actuar en consecuencia y evitar el drama humanitario: "Deberíamos haberlo sabido", resumía la autora (Novack, 2015).

Al margen de su uso para pronosticar posibles ataques, el Big Data tiene otras aplicaciones en la ciberguerra sobre las que volveremos más adelante, como el "aprendizaje" de robots, la cibervigilancia o, incluso, la selección de objetivos para un ataque con drones.

Las fechas de la ciberguerra

No es muy conocido que el primer ensayo de guerra cibernética se produjo en Vietnam (Shaw, 2016). Entonces, parecía un buen plan. Entre el 16 y el 25 de junio de 1966, un grupo de científicos de elite, principalmente físicos, denominados "Los Jason" en honor del héroe griego que lideró a los Argonutas (la idea fue de la mujer de uno de ellos), se reunieron en un edificio custodiado día y noche en Wellesley, Massachusetts: el señorial Dana Hall School, un selecto colegio privado femenino. Su misión era analizar el desarrollo de la guerra de Vietnam hasta el momento y presentar alternativas. Sus conclusiones se plasmaron en un informe de finales de agosto, entregado al secretario de Defensa, Robert McNamara. En el mismo, los expertos tachan de fracaso la campaña de bombardeos y proponen, en cambio, la creación de dos barreras defensivas. Se trataría de una sofisticada red de sensores electrónicos, aviones no tripulados y equipos que detectasen los movimientos del enemigo en el bosque y que fuese capaz de desencadenar una respuesta automatizada de ataque, lo que el Comité de Defensa del Senado llamaría después "campo de batalla electrónico". La operación fue aprobada e incluyó el despliegue de los Lightning Bug, los primeros drones usados en una guerra.

Igloo White fue el nombre en clave que se asignó a la segunda línea defensiva ideada por Los Jason, también conocida como "Línea McNamara". Se trataba de una barrera virtual con sensores electrónicos (acústicos, térmicos, químicos…) ideados para, teóricamente, rastrear de forma remota el movimiento de las tropas enemigas a través de Laos y Vietnam. Cuando un sensor detectaba un estímulo —como el sonido de un camión, una vibración en el suelo, el "olor" de un soldado, o incluso un cambio en la luz—, emitía una señal de radio a receptores cercanos de tierra y aire, incluyendo a los Lockheed EC-121, aviones de detección y vigilancia. Estas señales eran transmitidas a la base de vigilancia de Estados Unidos, en Nakhon Phanom (Tailandia). Este centro de

operaciones, de 20.000 pies cuadrados, conocido como Grupo de Trabajo de Alfa, fue el centro neurálgico de Igloo White y contaba con alrededor de 400 miembros de la Fuerza Aérea. Allí, dos superordenadores IBM 360-65 se encargaban del procesado de la información de los sensores de entrada. La cadena de sensores activados se mostraba iluminándose en un mapa de guerra en una pantalla instalada en una pared de sala. Estos patrones iluminados, que denominaban "gusanos", se utilizaron para determinar cuándo llegarían convoyes humanos y camiones a una determinada zona. Según un experto, "el piloto de estos aviones ni siquiera tenía que darle al botón que dejaba caer las bombas, porque en Igloo White el ataque estaba automatizado según los movimientos seleccionados por la computadora". Así, la guerra de Vietnam fue la primera "tecnoguerra" de la historia en la que se luchó "tanto con hojas de cálculo y estadísticas como soldados y bombas" (Shaw, 2016).

La Operación Igloo White no salió a la luz hasta la revelación, en The New York Times, de los "Papeles del Pentágono", los documentos secretos filtrados por el exanalista Daniel Ellsberg, que demostraban la verdadera cara de aquella guerra y que el periódico empezó a publicar, en primera página, el 13 de junio de 1971. Asimismo, se conocerían las críticas a la campaña: "En el momento en que la tecnoguerra alcanza su cima tecnológica, se convierte por completo en una representación", se dijo. Y es que "de principio a fin, el enemigo del campo de batalla electrónico existía solo como una señal de fondo generada por sensores remotos" (Shaw, 2016). Igloo White se dirigía desde "un sofisticado recinto de radio que creaba un ambiente autorreferencial de algoritmos informáticos, helicópteros de combate automatizados y gusanos electrónicos". En 1972, Eric Herter, un veterano estadounidense de la guerra de Vietnam, afirmó que el campo de batalla electrónico era "una máquina de muerte mecánica". Críticas muy cercanas a las que hoy se dirigen contra las operaciones con drones (Tenold, 2016).

La estrategia terminó siendo un fracaso desde el punto de vista técnico, militar y humanitario. Los sensores, entre otros problemas, no tenían la precisión prevista; la "barrera electrónica", con menos cobertura de la que se pensaba, no fue capaz de detectar movimientos relevantes de las tropas vietnamitas ("nuestras estimaciones fueron erróneas", se dijo en un informe que evaluó

años después la operación); y, como era de esperar, provocó innumerables muertes de civiles.

Por otro lado, su coste fue desproporcionado: Igloo White costó alrededor de mil millones de dólares al año. El coste de las operaciones de bombardeo basadas en la información de los sensores ascendió aproximadamente a 18,2 millones de dólares por semana, además de los cientos de aviones perdidos durante las campañas o las tripulaciones que los pilotaban. Los estudiosos de hoy siguen divididos sobre los méritos del sistema de barrera electrónica y la eficacia de las campañas bombardeo que dirigió (Shaw, 2016). Desde entonces, el desarrollo de la ciberguerra ha ido parejo a la expansión de la informática y, con ella, a la explotación de sus vulnerabilidades.

El 1988, se produjo una de las primeras incidencias en este sentido de alcance global: el gusano Morris, denominado así por el nombre de su creador, Robert Morris Tapan, la primera persona condenada por la ley estadounidense de fraude y abuso informático (Computer Fraud and Abuse Act), aprobada entonces dos años atrás. Morris es hoy profesor del MIT (Massachusetts Institute of Technology).

El gusano Morris fue uno de los primeros virus reconocidos que afectó a la entonces incipiente infraestructura cibernética mundial. El gusano utilizaba debilidades en el sistema UNIX y se replicaba a sí mismo con regularidad. De este modo, ralentizaba los ordenadores hasta hacerlos inutilizables. Los expertos en seguridad informática actuales confirman su relevancia: “Este caso prehistórico es realmente muy importante, ya que combina DDoS, exploits, tecnologías furtivas, fuerza bruta y otras técnicas que se utilizan ahora ampliamente en el malware moderno” (Malenkovich, 2013). Su notoriedad fue tal que su código fuente se conserva en un disquete que se exhibe en el Museo de la Ciencia de Boston.

Dejando atrás estos precedentes, en el siguiente cuadro se pueden ver las fechas clave de la ciberguerra actual.

Cronología de la Ciberguerra[38]

2003 Estados Unidos aprueba su Estrategia Nacional para la Seguridad del Ciberespacio[39].

2006 Mayo. Un intruso accede a las redes del Departamento de Estado norteamericano, según se dijo, "descargando terabytes de información".

Agosto. Un oficial de la Fuerza Aérea declara que "China se ha descargado de 10 a 20 terabytes de datos de la SIPRNet (la red militar no clasificada)".

Diciembre. La NASA se vio obligada a bloquear mensajes de correo electrónico con archivos adjuntos antes de una misión espacial. Business Week informó de que "intrusos extranjeros desconocidos habían obtenido los planes de las últimas lanzaderas espaciales".

En algún momento de 2006, el entonces presidente norteamericano George Bush autorizó el desarrollo de "ciberarmas" para emplear contra las instalaciones nucleares de Irak. No se sabrá hasta 2012, por una información de The New York Times.

Malasia adopta su Estrategia Nacional de Ciberseguridad[40].

2007 Marzo. Test del Generador Aurora. El Laboratorio Nacional de Idaho realiza una prueba para demostrar cómo un ataque cibernético podría destruir los componentes físicos de la red eléctrica, haciéndolos explotar.

Abril. Primer ataque por denegación (DDoS) en la historia contra un Estado. Las redes del Gobierno de Estonia (en aquel momento, uno de los países con mayor infraestructura digital) sufren un ataque de denegación de servicio. El ataque se atribuye a Rusia por la eliminación de un monumento a los caídos. Algunos servicios en línea del Gobierno quedaron interrumpidos temporalmente y la banca online se paralizó, aunque la mayoría de los sitios atacados quedaron operativos de nuevo pocas horas después. Los cables de WikiLeaks publicados en 2011 desvelaron que habría sido un ataque de

Rusia tratando de probar una nueva arma: una botnet (red de robots informáticos o bots, que se ejecutan de manera autónoma y automática, y se controlan de forma remota) "alquilado".

Junio. Ataque a las redes no clasificadas del Pentágono, incluyendo el acceso a la cuenta de correo del secretario de Defensa norteamericano.

Agosto. Alemania, Francia y Reino Unido denuncian que grupos procedentes de China se han infiltrado en sistemas críticos de información gubernamentales.

Octubre. China informa que hackers extranjeros —según afirmaba, el 42 por ciento procedían de Taiwán y el 25 por ciento de Estados Unidos— habían robado información de las áreas clave del Gobierno.

2008 Enero. Symantec identifica el virus Trojan.RandsomC, el primer malware puro de bloqueo de equipos usado para ataques de ransomware (secuestro de sistemas que se "liberan" a cambio de una recompensa económica).

Abril. Según uno de los cables filtrados por WikiLeaks, piratas informáticos habrían robado con éxito "50 megabytes de mensajes de correo electrónico, documentos adjuntos, así como una lista completa de nombres de usuario y contraseñas de una agencia del Gobierno norteamericano no especificada. El ataque se atribuye a un grupo de hackers con sede en Shanghái.

Agosto. Redes de ordenadores de Georgia son atacadas cuando el país se encuentra en mitad de un conflicto con Rusia. Se producen desfiguraciones de webs, pero hubo poca o ninguna interrupción de los servicios.

Noviembre. Las redes clasificadas del Departamento de Defensa norteamericano sufren un ataque con software malicioso (el virus Agent.btz), que llevó a prohibir el uso de dispositivos extraíbles (pen drives) en cualquier equipo del Ejército. El incidente se dio a conocer como "el peor ciberataque de la historia" y dio pie a la

creación del Mando Cibernético vinculado a la NSA.

2009 Enero. Ataque a la infraestructura de Internet de Israel durante la ofensiva militar en la Franja de Gaza. El ataque, que se centró en los sitios web del Gobierno, fue ejecutado por al menos cinco millones de ordenadores. Los funcionarios israelíes afirmaron que el ataque fue llevado a cabo por una organización delictiva con base en un antiguo Estado soviético y pagado por Hamas o Hezbolá.

Julio. Ataques de denegación de servicio (DDoS) durante varios días contra sitios web de Estados Unidos y Corea del Sur, incluyendo webs del Gobierno. Corea del Sur acusó a Corea del Norte de estar detrás de estas acciones.

2009 Australia adopta su Estrategia de Ciberseguridad[41].

2010 Enero. Operación Aurora. Google anunció que un sofisticado ataque había penetrado en sus redes, además de las de otras 30 empresas de Estados Unidos. Entre ellas, la compañía de servicios financieros Morgan Stanley. El ataque se atribuye a China.

Enero. Un grupo que se hace llamar el "Ciberejército Iraní" interrumpe el servicio del motor de búsqueda chino Baidu. Los usuarios se redirigen a una página que muestra un mensaje político iraní. El mismo grupo había hackeado Twitter el mes de diciembre anterior con un mensaje similar.

Abril. Se cree que hackers chinos irrumpen en archivos clasificados del Ministerio de Defensa indio y embajadas indias en todo el mundo, teniendo acceso a información sobre sus sistemas de armamento y de misiles.

Junio. Stuxnet, una pieza compleja de software malicioso diseñado para interferir con los sistemas de control industrial de Siemens, fue descubierto en Irán, Indonesia y otros lugares. Más tarde se supo que se trataba de un arma cibernética de Estados Unidos e Israel dirigida contra el programa nuclear iraní.

Diciembre. La web de la Oficina Central de Investigaciones India (CBI) es hackeada y se borran datos. India culpa a hackers paquistaníes. La información sensible, almacenada en equipos no fácilmente accesibles a través de Internet, no se vio afectada.

A lo largo de 2010. Estonia, Bulgaria, Eslovenia, Canadá, Reino Unido y Mongolia aprueban o ponen en marcha estrategias de ciberseguridad[42].

2011 Enero. El Gobierno de Canadá informó de un ataque cibernético importante contra algunos de sus organismos, incluyendo la agencia de investigación del Departamento de Defensa Nacional de Canadá. El ataque obligó a desconectar de Internet a los principales organismos económicos del país.

Enero-marzo. Ataque de los servicios de espionaje británicos (GCHQ) contra la empresa de telefonía belga Belgacom. La intrusión no saldría a la luz hasta 2013, gracias a los papeles de Snowden.

Abril. Hackers, utilizando técnicas de phishing, obtuvieron información que comprometería la tecnología de autenticación SecurID de la empresa RSA, usada por agencias gubernamentales y servicios financieros, entre otros.

Abril. Google informó de un ataque por phishing que habría permitido el acceso a cientos de correos de Gmail y contraseñas de las cuentas de personas prominentes, entre ellos altos funcionarios de Estados Unidos. Google atribuyó el ataque a China.

Mayo. Piratas informáticos que se hacen pasar por miembros del grupo hacktivista Anonymous penetraron en la red PlayStation. Sony estimó que datos personales (incluyendo datos bancarios) de más de 80 millones de usuarios se vieron comprometidos y valoró el coste del ataque para la compañía en más de 170 millones de dólares.

Septiembre. La Universidad de Tecnología y Economía de Budapest descubre Duqu, una colección de malware

relacionado con el gusano Stuxnet. Al igual que este, Duqu ataca los sistemas Microsoft Windows utilizando una vulnerabilidad de día cero. Los servidores estaban dispersos en diferentes países, entre ellos Alemania, Bélgica, Filipinas, India y China.

Septiembre. Un virus informático de una fuente desconocida introdujo malware del tipo keylogger en las estaciones de control en tierra de vehículos aéreos no tripulados (drones) de las Fuerzas Aéreas norteamericanas.

A lo largo de 2011. Países como Alemania, Reino Unido, Lituania, Luxemburgo, Holanda, Corea del Sur, Uganda o Colombia aprueban sus estrategias de ciberseguridad.

2012 Enero. Primer vuelo con éxito de X-47B, el primer dron autónomo (no pilotado a distancia), capaz de aterrizar por sí mismo en la cubierta de un portaviones y que la Marina norteamericana había estado probando desde 2011. Estará destinado a labores de vigilancia y, a diferencia de los Predator (en uso desde los años noventa), no estará armado.

Octubre. La empresa rusa Kaspersky descubre un ataque cibernético en todo el mundo llamado Octubre Rojo, que había estado funcionando al menos desde 2007. Los hackers reunieron información a través de vulnerabilidades en los programas Word y Excel de Microsoft. Los objetivos principales de los ataques fueron los países de Europa del Este, la ex Unión Soviética y Asia Central, aunque en Europa Occidental y América del Norte también se reportaron incidentes. El virus accedió a información de embajadas, empresas de investigación, instalaciones militares, proveedores de energía, centrales nucleares y otras infraestructuras críticas.

Marzo. La BBC informó de un "sofisticado ataque cibernético" que incluyó intentos de interrumpir la transmisión de los satélites por los que emiten en este país. Acusó a Irán.

Marzo. El Departamento de Seguridad Nacional de Estados Unidos decretó alerta amarilla por una campaña de intrusión cibernética en las tuberías de gas del país desde diciembre de

2011. Se describió el ataque como una sofisticada acción de phishing lanzada por una sola fuente.

Abril. Irán tuvo que desconectar sus instalaciones de petróleo principales después de un ataque cibernético contra sus sistemas informáticos internos. La producción de petróleo no se vio afectada, pero sí los sitios web del Ministerio de Petróleo iraní y de la compañía nacional de petróleo. El origen del ataque fue el virus Wiper, que se atribuye a Israel.

Mayo. Un conjunto de herramientas de espionaje denominado "Flame" se descubre en los equipos del Ministerio de Petróleo de Irán, así como en otros países de Oriente Medio (incluidos Israel, Siria y Sudán) y del resto del mundo.

Agosto. El mismo malware, también apodado "Gauss", infecta a 2.500 sistemas en todo el mundo. Aparentemente, iba dirigido contra bancos libaneses.

Agosto. Un grupo llamado Cutting Sword of Justice, vinculado a Irán, utiliza el virus Shamoon para atacar Aramco, un importante proveedor de petróleo de Arabia Saudita, borrar datos de 30.000 equipos e infectar (sin causar daños) sistemas de control. El ataque también afectó a la empresa catarí RasGas, entre otras compañías de hidrocarburos.

Septiembre. Izz Ad-Din Al-Qassam, un grupo de hackers vinculados a Irán, lanza la Operación Ababil, focalizada en sitios web bancarios y las principales instituciones financieras de Estados Unidos.

Septiembre. Telvent, fabricante de un sistema de control industrial, informa que unos hackers habían atacado su red, accediendo a archivos relacionados con un sistema utilizado en partes de la red eléctrica.

Octubre. Seis grandes bancos estadounidenses sufren interrupciones en el servicio después de ataques de denegación de servicio por Izz Ad-Din Al-Qassam, Las autoridades estadounidenses sugieren la participación iraní.

A lo largo de 2012. Noruega, Suecia, Georgia, Jordania, Sudáfrica y Trinidad y Tobago adoptan sus estrategias de ciberseguridad[43].

2013 Enero. Izz Ad-Din Al-Qassam, el ala militar que se vincula a Hamas, reivindica nuevos ataques de denegación de servicio contra web financieras de Estados Unidos, como parte de la Operación Ababil.

Enero. El Ministerio de Asuntos Exteriores japonés sufre un ciberataque y pierde "al menos" veinte documentos, algunos de alto secreto.

Enero. Medios norteamericanos como The Nueva York Times, Wall Street Journal, The Washington Post y Bloomberg News revelan que habían sido víctimas de ataques cibernéticos persistentes, presumiblemente procedentes de China.

Febrero. Der Spiegel revela que EADS (European Aeronautic Defense and Space Company) y la siderúrgica alemana ThyssenKrupp registraron grandes ataques de piratas informáticos chinos en 2012.

Febrero. El Departamento de Seguridad Nacional revela que, desde diciembre de 2011 hasta junio de 2012, piratas informáticos dirigieron ataques contra 23 empresas de gasoductos y robaron información que podría ser utilizada para el sabotaje.

Marzo. Estaciones de televisión de Corea del Sur e instituciones financieras son golpeadas con un ataque cibernético que, se cree, se originó en Corea del Norte, con el malware diseñado para evadir un software antivirus Corea del Sur.

Marzo. La empresa de seguridad Kaspersky identifica un malware espía, Turla, con semajanzas con Agent.btz, Octubre Rojo y Flame/Gauss.

Abril. Operación Israel. Ataque cibernético coordinado contra sitios web de Israel, en protesta por sus acciones contra el pueblo palestino, a través de ataques de denegación del

servicio, secuestro y filtraciones de bases de datos, control del panel de administración y desfiguraciones. El ataque se atribuye a Anonymous.

Mayo. Las autoridades israelíes informan de un intento fallido del Ejército Electrónico Sirio de comprometer el suministro de agua a la ciudad de Haifa.

Junio. Edward Snowden, exanalista de la NSA, revela documentos que muestran, entre otras cosas, que Estados Unidos realiza espionaje cibernético contra objetivos europeos, China, Rusia, Brasil, incluyendo el espionaje masivo de los sistemas nacionales de telecomunicaciones.

Agosto. Un ataque DDoS masivo hace caer el dominio .cn de China durante varias horas.

Agosto. El Ejército Electrónico Sirio secuestra y desvía las principales redes sociales y los medios de comunicación occidentales a un sitio de alojamiento malicioso en Rusia.

Agosto. Hackers iraníes acceden al sistema SCADA (sistema de control automático) de una presa en el Estado de Nueva York. La noticia no saldría a la luz hasta diciembre de 2015.

Septiembre. Hackers brasileños, irritados por las revelaciones sobre la vigilancia de la NSA, desfiguran la página web de la NASA por error.

Marzo. Instituciones financieras de Corea del Sur y el organismo público de radiodifusión sufren ataques en sus redes, que atribuyen a Corea del Norte.

Mayo. Un dron Predator 107 (P107) alcanza el récord de 20.000 horas de vuelo en un solo avión. El hito fue alcanzado en el desempeño de una misión de combate de 21 horas en apoyo de la llamada Operación Libertad Duradera en Afganistán. La Fuerza Aérea comenzó a usar los Predator para labores de reconocimiento en los Balcanes en los 90, pero después fue armado con misiles y ha intervenido entre otras operaciones, en las guerras de Irak y Afganistán. La CIA

también usó Predator en operaciones en Pakistán y Yemen.

Junio. Primera reunión sobre defensa cibernética de los ministros del ramo de la OTAN. Acuerdan crear un Mando Conjunto para este nuevo "dominio".

Diciembre de 2013. El Banco Central de China se ve afectado por ataques DDoS. Los medios estatales chinos señalan como autores a usuarios de Bitcoin, enojados por las nuevas regulaciones del país asiático en este terreno.

A lo largo de 2013. Hungría, Italia, Polonia, Portugal, Rumanía, España, Turquía, Austria, Chipre, Finlandia, Montenegro, India, Singapur, Egipto, Marruecos, Zimbawe y Panamá adoptan sus estrategias de ciberseguridad nacionales. La Unión Europea adopta su estrategia conjunta de ciberseguridad[44].

2014 Marzo. Fuentes de Defensa de la India admiten que material clasificado habría quedado comprometido por un ataque en 50 equipos de las fuerzas armadas y la organización de investigación de Defensa.

Abril. Se da a conocer la vulnerabilidad Heartbleed, considerada como "el mayor fallo de seguridad en Internet", con un importante agujero de seguridad en las librerías OpenSSL, ampliamente utilizadas en los servicios de cifrado en las comunicaciones por la red. Esta vulnerabilidad habría permitido obtener información sensible de los sistemas afectados al "romper" el cifrado en las comunicaciones. Se piensa que la NSA conocía y había explotado esta vulnerabilidad, sin haberla reportado, lo que provoca críticas unánimes de la comunidad informática mundial.

Junio. La empresa de seguridad Symantec da a conocer Dragonfly, una amenaza avanzada o APT, dirigida especialmente contra sistemas de control industrial en el sector energético en Europa, aunque también se detectó en el farmacéutico. A partir de un sistema de acceso remoto RAT (Remote Access Tool) se infectaban y controlaban remotamente los equipos afectados.

Agosto. Sale a la luz, Machete, otra APT (amenaza avanzada), pero de habla hispana, con expresiones en castellano dentro de su código. Estaba activa desde 2010 y se dirigía especialmente a servicios de inteligencia, militares y organizaciones gubernamentales de países latinoamericanos. La dio a conocer la empresa de seguridad Kaspersky.

Agosto. Sale a la luz una campaña de ciberespionaje dirigida a miembros del Gobierno y diplomáticos de países de Europa del Este, mediante el virus Turla.

A lo largo de 2014. Albania, Dinamarca, Estonia, Islandia, Letonia, Lituania, Afganistán, Bangladesh, Pakistán, Emiratos Árabes, Nigeria, Ghana, Kenia y Mauritania adoptan sus estrategias de ciberseguridad[45].

2015 Enero. Robo de 5 millones de dólares en bitcoins sufrido por Bitstamp, el tercer intercambiador de la divisa virtual a nivel mundial. La brecha de seguridad en sus sistemas produjo la sustracción de 19.000 monedas digitales y obligó a la suspensión de su servicio unas 24 horas.

Enero. Ciberataques contra más de 19.000 páginas web francesas tras el atentado contra la revista satírica Charlie Hebdo. Algunos ciberataques fueron realizados por grupos conocidos de piratas informáticos islámicos afiliados al grupo terrorista ISIS. También se vieron afectadas las páginas web de 60 ayuntamientos de Navarra, cuyo proveedor de servicios está en Francia.

Enero. Las cuentas del Ejército estadounidense en Twitter (@centcom) y YouTube fueron infiltradas por piratas informáticos que alegaron haber actuado bajo las directrices del Estado Islámico, cambiando las imágenes del perfil de la cuenta y publicando mensajes de apoyo al yihadismo. Defensa explicó en un comunicado que la seguridad de las dos páginas estuvo "comprometida" durante cerca de 30 minutos, por lo que lo definen como un acto de "vandalismo cibernético". El supuesto autor de la acción, un yihadista británico de 21 años, fue eliminado mediante un ataque con drones dirigido por el Ejército norteamericano en agosto de 2015.

Febrero. Desmantelamiento de la botnet Ramnit, una red de máquinas activa desde 2010 que había infectado aproximadamente 3,2 millones de ordenadores de todo el mundo. La Europol dirigió una operación conjunta en la que participaron agencias de Alemania, Holanda, Italia y Reino Unido, en colaboración con las compañías AnubisNetworks, Microsoft y Symantec. Como resultado, se apagaron los servidores de comando y control de la botnet y se redirigieron un total de 300 dominios de Internet.

Abril. Ciberataque sufrido por TV5Monde, así como su sitio web y su página de Facebook, que se utilizaron para hacer apología del terrorismo yihadista. La programación se suspendió hasta que se recuperó el control.

Abril. Caída de la botnet SIMDA, que habría infectado a más de 770.000 ordenadores de más de 190 países, distribuyendo varios tipos de virus, entre ellos troyanos financieros y software ilícito. Se lograron intervenir 10 servidores de comando y control.

Julio. Seis lanzaderas y dos radares Patriot alemanes, desplegados en Turquía cerca de la frontera con Siria, habrían ejecutado una serie de órdenes desconocidas durante un periodo de tiempo limitado. Supuestamente, estas órdenes eran emitidas por una "fuente extranjera desconocida", según informaron medios alemanes desmentidos por el Gobierno.

Agosto. Ataques por organizaciones islamistas y yihadistas contra organizaciones gubernamentales de Estados Unidos, que provocaron una desfiguración en la web de Ejército, la fuga de datos de más de 4 millones de usuarios de la Administración federal o el acceso fraudulento a más de 100.000 cuentas tributarias de usuarios estadounidenses.

A lo largo de 2015. República Checa, Francia, Eslovaquia, Irlanda, Serbia, Japón, Gambia, adoptan sus estrategias de ciberseguridad[46].

2016 Enero. Un ataque con un malware denominado "Black-Energy" provoca un apagón que afecta al menos a 80.000

usuarios en una región del oeste de Ucrania. Los expertos describen el incidente como el primer corte de energía conocido causado por un ataque cibernético.

Febrero. El secretario de Defensa estadounidense solicita al Congreso un aumento del presupuesto en investigación militar de cara a 2017, destinado principalmente a la Oficina de Capacidades Estratégicas (SCO), inmersa en el desarrollo de diferentes proyectos que tienen que ver con la autonomía robótica.

Marzo. El Gobierno español prevé que, a lo largo de 2016, los ciberataques asciendan a 100.000. De ellos, 300 serían contra infraestructuras críticas.

2016. Eslovenia y Ucrania adoptan sus estrategias de ciberseguridad[47].

Capítulo 4

Todos los secretos de la primera arma cibernética

Creo que los virus informáticos deberían contar como vida. Creo que dice algo acerca de la naturaleza humana que la única forma de vida que hemos creado hasta ahora sea puramente destructiva.

Stephen Hawking

Cuando se trata de ciberespacio, el mundo conectado está viviendo en una casa de cristal, y todos sabemos que la gente en casas de cristal no debería arrojar piedras.

Haroon Meer (2013)

Si alguien le preguntase a Sergey Ulasen[48], ingeniero informático de poco más de 30 años, cómo disfruta más, diría que en el campo en casa de su abuela en una pequeña localidad rural de Bielorrusia. Sin cobertura móvil y con tranquilidad para "ordenar la cabeza".

Sin embargo, cuando no está allí, Sergey no desaprovecha un minuto. Cada vez que tiene un momento libre, trata de hacer algo "que valga la pena" porque cree que las personas "deben desarrollarse continuamente a sí mismas". Por ejemplo, si ve una película americana, Sergey conecta el audio original para practicar su comprensión en inglés. Y el rato que tarda en llegar a la oficina lo utiliza para escuchar podcasts, programas de formación y literatura extranjera.

Por eso, tal vez mantenga ese aspecto espigado y vivo. Pero Sergey, rubio y con el pelo muy corto, barbilampiño, piel blanquísima, de mirada tranquila, sonrisa tímida y vestimenta informal —vaqueros y camisetas de gusto variable—, tiene sobre todo la imagen de quien nunca se mete en líos. Detesta las películas de terror y tampoco es fan de las de intriga.

De modo que, con este perfil, cuesta imaginarle en el centro de uno de los episodios más inquietantes de la ciberguerra moderna. Sergey se graduó en 2006 en la Universidad Técnica de Bielorrusia como desarrollador de software. Comenzó su carrera profesional en una pequeña empresa local de seguridad informática, VirusBlokAda, donde se unió al equipo que diseñó el motor antivirus de la compañía. Allí se dedicaba al desarrollo de software, análisis de amenazas y consultoría técnica. También a hacer frente a los incidentes relacionados con el malware que reportaran sus clientes. Esto iba a hacer que su rutina cambiase a principios del verano de 2010.

Una boda y la Pantalla Azul de la Muerte

"Todo comenzó cuando los chicos de soporte técnico me informaron sobre un caso bastante inusual: un cliente en Irán reportó una BSOD y el reinicio del equipo de forma arbitraria. Me remitieron una solicitud de ayuda junto con sus informes preliminares de exploración", recordaría más tarde un Ulasen ya famoso.

La incidencia llamada BSOD (Blue Screen of Death, más conocida en castellano como "pantalla azul de la muerte" o "pantalla azul")[49], hace referencia a la pantalla mostrada por el sistema operativo Windows de Microsoft cuando no puede, o está en peligro de no poder, recuperarse de un error del sistema. Ocurre cuando el núcleo del sistema operativo no puede recuperarse de un error y la única acción que un usuario puede realizar es reiniciar el sistema perdiendo todo el trabajo no guardado, el estado de todos los programas ejecutándose en ese momento y peligrando la integridad del sistema de archivos.

La información que aparece en la pantalla azul de la muerte muestra lo que estaba haciendo el procesador en el momento del error, pero no suele servir para conocer la fuente del problema, haciendo que la detección del fallo sea muy difícil, por no decir imposible. En el peor de los casos, como dice en la misma pantalla azul, la unidad del dispositivo se estanca en un bucle infinito: cada vez que se enciende el PC aparece la pantalla azul, se reinicia sola o, si no, al reiniciarla el usuario, vuelve a aparecer la pantalla azul, y así sucesivamente.

La primera impresión de Sergey Ulasen fue que las anomalías encontradas eran debido a algún error de configuración de Windows o resultado de un conflicto entre las aplicaciones instaladas, lo que es bastante común. Por ello, recomendó que el departamento de soporte técnico consiguiera la máxima información posible sobre las aplicaciones instaladas. Sin embargo, no tardaría en darse cuenta de que no se trataba de un simple

problema de mal funcionamiento del equipo. Cuando supo que las mismas anomalías se habían encontrado en muchos otros ordenadores de la red del cliente, incluso en algunos con una instalación nueva de Windows, y que habían pasado exhaustivas pruebas contra aplicaciones basura, Sergey ya no tuvo duda de que el incidente guardaba relación con una infección por malware y que sería probablemente un rootkit, ya que no lo habían podido detectar con los métodos habituales (antivirus). Sin duda, había sido diseñado y construido por expertos.

Aunque pueden tener otras funciones, los rootkit[50] se asocian principalmente al malware, ya que permiten un acceso de privilegio a la administración del sistema operativo, pero mantienen su presencia activamente oculta, por ejemplo, deteniéndose cuando se produce un escaneo. Una vez que se instala un rootkit, no se puede confiar en ninguna información que el PC da sobre sí mismo. Así, si se le preguntara sobre todos los programas que se están ejecutando, el rootkit puede eliminar sigilosamente cualquiera de ellos del que no quiere que sepamos.

El cliente afectado por la "infección" era un ingeniero de Irán. Por suerte, no solo era un experto en seguridad con experiencia, sino también un buen amigo de Ulasen. En primer lugar, trató de resolver el asunto por sí mismo y luego con la ayuda del soporte técnico de VirusBlokAda. No consiguieron ningún resultado. Entonces llamó a Sergey. En Irán era un sábado soleado y día de trabajo. Mientras, en una Bielorrusia cubierta por las nubes, Sergey estaba en la boda de un amigo, a unos 400 kilómetros de Minsk, la capital. Entre invitados, celebrando, bailando y bebiendo, Ulasen se mantenía pegado al móvil dando soporte técnico ("y ¡psicológico!") a su amigo de Irán. Después de un rato, se dieron cuenta de que no podían hacer más progresos a través del teléfono y decidieron continuar con la investigación pasado el fin de semana.

Llegó el lunes por la tarde y, tras resolver algunos problemas técnicos para conseguir el acceso remoto al ordenador infectado, lograron dar con la causa de las anomalías. Finalmente, habían encontrado el malware y se dieron cuenta de su naturaleza furtiva, su extraño propósito y sus técnicas de propagación, a través de memorias USB infectadas.

Analizado el código por el equipo de VirusBlokAda, resultó que estaba utilizando vulnerabilidades de día cero (aquellas que no son todavía conocidas por el fabricante, aún no han sido "parcheadas" y, en general, no son detectadas por los programas antivirus), lo que le había permitido penetrar en ordenadores Windows aunque estuvieran adecuadamente actualizados. Esto les hizo dudar también de la autenticidad del certificado digital que el programa poseía. Un certificado digital es una especie de "pase" otorgado por una entidad externa que usan los programas y aplicaciones para garantizar (al equipo) que se puede confiar en ellos. Todos estuvieron de acuerdo en que el certificado digital debía de haber sido robado.

Esto, junto con la complejidad del código y las sofisticadas tecnologías rootkit que empleaba, les llevó a pensar que se trataba de un malware sin nada que se le pareciera en el mundo, por lo que era necesario informar a la industria y a la comunidad de seguridad informática de los detalles lo antes posible.

"Se dio cuenta de que estaba usando una vulnerabilidad de día cero para extenderse. Los días cero son las armas más potentes del mundo de la piratería: se aprovechan las vulnerabilidades de software que aún son desconocidas para el fabricante o los proveedores de antivirus. También son muy poco frecuentes; se necesita mucha habilidad y persistencia para encontrar este tipo de vulnerabilidades y explotarlas. De los más de 12 millones de piezas de malware que los investigadores de antivirus descubren cada año, menos de una docena utiliza un día cero" (Zetter, 2011c).

En un primer momento, decidieron informar solo a las partes involucradas: Microsoft y Realtek (la compañía que firmaba el certificado digital). Sin embargo, cuando lo hicieron, no recibieron ninguna respuesta. Al fin y al cabo, ¿qué posibilidades tenían de que una alerta de una pequeña empresa de antivirus bielorrusa tuviera alguna repercusión en una gran compañía?

Entonces, Sergey decidió darlo a conocer y notificar la incidencia abiertamente. El 12 de julio publicó algunos detalles sobre el malware, al que bautizó como "Rootkit.TmpHider" en el sitio web de VirusBlokAda (2010) y en un foro popular del sector, wilderssecurity.com.

En su post, Sergey explicaba que se trata de un troyano con funcionalidades de rootkit para ocultar su presencia en el sistema y que se propagaba fundamentalmente mediante dispositivos USB sin hacer uso del tradicional autorun.inf. Es decir, que tan solo utilizando un explorador de ficheros que visualizara los iconos era suficiente para infectar el equipo. Además, alertaba que el virus usaba drivers firmados digitalmente por Realket, lo que hace al troyano más ofensivo, puesto que los equipos lo considerarían confiable.

El post de Sergey[51] generó, como era de esperar, muchos comentarios. El joven ingeniero confiaba en llegar así a las principales empresas de antivirus y que, a través de ellas, Microsoft tuviera conocimiento de la vulnerabilidad detectada en su sistema operativo: “Hemos escrito a Microsoft, pero no nos han contestado. Creo que los principales vendedores de antivirus sí han prestado atención a este aviso y espero que ellos informen también a Microsoft y Realtek del problema”, escribió en el mismo foro dos días después. Entre las respuestas que se produjeron hubo una especialmente transcendente.

Los sistemas SCADA y la reunión secreta de Obama

El 14 de julio, Frank Boldewin, un ingeniero alemán independiente, publicó en el foro el siguiente comentario[52]: “Hola, chicos, ¿ha echado alguien ya un vistazo más profundo al malware? Me encontré con cosas como esta después de descifrar algunas etapas de la muestra MD5 016169ebebf1cec2aad6c7f0d0ee9026”. Y copiaba unas líneas del código descifrado que mostraban que el virus se dirigía contra algún tipo de equipo de Siemens.

Figura 3

Fragmento del código del virus entonces llamado Rootkit.TmpHider

Code:

```
SOFTWARE\Microsoft\MSSQLServer
pd1
Grac5\
2W5Xcder
WinCCConnect
master
.\WinCC
sqloledb
Grac5\cc_tlg7.sav
Step7\Example
use [%s]
declare @t varchar(4000), @e int, @f int if exists (select text from dbo.syscomments where id=object_id(N'[dbo].[MCPVR
declare @t varchar(4000), @e int, @f int if exists (select * from dbo.syscomments where id=object_id(N'[dbo].[MCPVPRO]
use master
select name from master..sysdatabases where filename like N'%s'
exec master..sp_attach_db 'wincc_svr',N'%s',N'%s'
exec master..sp_detach_db 'wincc_svr'
use wincc_svr


or

SOFTWARE\SIEMENS\WinCC\Setup
STEP7_Version
SOFTWARE\SIEMENS\STEP7
SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation
NTVDM TRACE
.MCP
.zip
~DT
%s\WINCC
```

Boldewin concluía: “Esto me apunta al sistema SCADA WinCC de Siemens. Parece que este malware se hizo para el espionaje”.

SCADA, acrónimo de Supervisory Control And Data Acquisition (“Supervisión, Control y Adquisición de Datos”), es un software que permite controlar y supervisar procesos industriales. El término usualmente se refiere a un sistema central que monitoriza y controla un sitio completo (una planta industrial, normalmente) o una parte del mismo (depósitos, bombas, etc.).

El sistema SCADA está compuesto por un software y por diferente hardware de manejo de señales entrada (sensores) y salida, “interfaces” (pantallas) entre el hombre y las máquinas (HMI), bases de datos, redes, comunicaciones y controladores. Es decir, se integran todas las máquinas y dispositivos existentes en una planta de producción, si se trata de una industria, o de las instalaciones, si se trata de otro tipo de infraestructura, como una central energética: autómatas programables (PLCs), motores, bombas, ventiladores, etc. En definitiva, todos los dispositivos que componen el sistema automatizado.

El sistema captura toda la información del proceso de producción, visualiza en tiempo real el estado de las máquinas y dispositivos, realiza análisis y mediciones e informa de alarmas configuradas, entre otras funciones. SCADA permite realizar retroalimentaciones al proceso en función de los datos obtenidos. Por ejemplo, si tenemos definido que el nivel de un depósito de agua no puede bajar del 50 por ciento de su capacidad, el sistema automáticamente detectará ese nivel y realizará las acciones oportunas para el llenado del mismo[53].

El post de Frank Boldewin iba a tener un gran alcance, puesto que descubriría por primera vez la conexión del virus con el control de procesos industriales. El virus, del que unos meses más tarde se descubriría que había infectado a más de 100.000 ordenadores en todo el mundo, mostraba tener una misión que hasta ahora no se había visto en ningún tipo de malware: “Es la primera vez que el malware conocido no va dirigido a obtener los datos de tarjetas de crédito o a tratar de robar datos personales del usuario, sino que está atacando sistemas de procesamiento en la vida real. Es por eso que es único, y no en términos exagerados”, diría Nicolas Falliere,

uno de los ingenieros de Symantec que analizaron el código del virus hasta llegar a los más insospechados secretos sobre su origen y naturaleza.

El 18 de julio, unos días después del comentario de Frank Boldewin, alguien que se presentaba como ingeniero de sistemas SCADA y exrrepresentante de los equipos de Siemens durante 25 años, tiraría de ese hilo en el mismo foro: se preguntaba si el único sistema señalado por el virus era de Siemens o si, por el contrario, también podrían ser "víctimas" del mismo otros sistemas de automatización que existen en el mercado con fines distintos a los industriales. En caso de ser Siemens —advertía el ingeniero—, cuya aplicación industrial es muy específica, invitaba a relacionar las zonas donde se habían detectado infecciones del virus (se acababa de conocer, por un informe de Symantec, que eran Indonesia, India e Irán) con el mercado de la empresa alemana. También llamaba la atención sobre el hecho de que un virus que afectaba a sistemas Siemens no tuviera presencia en Europa, siendo la región donde están más extensamente instalados. El círculo se iba cerrando.

La primera persona en publicar una información sobre el nuevo virus fue Brian Krebs, un periodista famoso en el ámbito de la seguridad informática, antiguo reportero de The Washington Post cuyo blog tenía muchos seguidores. Era 15 de julio. En su artículo, Krebs (2010) recoge tanto la naturaleza furtiva del malware, su propagación a través de USB, o el certificado digital con que contaba, como la posible relación con los sistemas SCADA. Explicaba que VirusBlokAda había descubierto que, al acceder a ellos mediante el Explorador de Windows, los accesos directos maliciosos eran capaces de ejecutarse de forma automática si están escritos en una unidad USB. "Por lo que solo tiene que abrir, con Explorer o cualquier otro gestor de archivos que puede mostrar iconos (por ejemplo, Total Commander), el USB infectado para infectar su sistema operativo y permitir la ejecución de los programas maliciosos", recogía Krebs citando a Sergey Ulasen.

"Si se trata realmente de una nueva vulnerabilidad en Windows, pronto se podría convertir en un método popular para la propagación de malware. Pero, por ahora, esta amenaza parece bastante dirigida: el investigador de seguridad independiente Frank

Boldewin dijo que tuvo la oportunidad de diseccionar las muestras de malware y observó que parecían estar buscando sistemas SCADA de Siemens WinCC, o máquinas encargadas del control de las operaciones de empresas grandes, tales como fábricas o centrales eléctricas", escribió Krebs.

Al día siguiente, Microsoft (2010) publicó una nota sobre la vulnerabilidad descubierta por VirusBlokAda. Andreas Marx, de la empresa de antivirus AV-test.org, había finalmente logrado alertar al equipo de incidencias de la compañía de Windows, el sistema operativo afectado por el virus, y se habían puesto a trabajar en ello. En su ficha sobre la alerta Microsoft, advierte que el fallo podría permitir la ejecución de código de forma remota. Les había llevado cuatro intensos días de trabajo a un equipo de más de 30 analistas llegar a descubrir todas las vulnerabilidades que explotaba el virus.

A partir de ahí, la información ya fue de difusión general. Se hicieron eco los medios y los equipos de respuesta ante emergencias informáticas (CERT), como el del organismo español sobre ciberseguridad, INCIBE (2010), que el 18 de julio publicaba una alerta sobre el virus. Y mientras esto ocurre en los círculos —de momento estrechos— de la seguridad informática, en el principal centro de toma de decisiones del mundo se trata de resolver un dilema: "¿Deberíamos parar esto?", pregunta gravemente Obama al equipo de crisis reunido en la sala de emergencias (la famosa Situation Room) de la Casa Blanca.

El presidente se reúne con un pequeño grupo encargado de darle la noticia. Ese día, en Washington, se alcanzaron los 39 grados; 2010 tuvo un mes de julio en el que se registraron temperaturas récord en la capital norteamericana, pero el ambiente en esta habitación de la Sala Oeste era gélido y tenso. La sala, estrecha, rodeada de pantallas y completamente securizada frente al rastreo de comunicaciones, está destinada al seguimiento de crisis desde su creación en la Administración Kennedy, en 1961.

Alrededor de una larga mesa de madera color caoba, estrecha y brillantísima, se sientan en sillones negros de piel reclinables Leon Panetta, jefe de la CIA en aquel momento, el general Cartwright, vicepresidente del Estado Mayor Conjunto de Estados Unidos, y

Michael J. Morell, el director adjunto de la CIA. Son los “jugadores principales” de una operación secreta denominada en clave “Juegos Olímpicos”, de la que no se sabrá nada, ni de esta reunión, hasta 2012, cuando The New York Times la saque a la luz a partir de testimonios de algunos de los participantes (Sanger, 2012).

Aunque el periódico no menciona el detalle, es más que probable que la reunión tuviera un testigo más: Bravo, la mascota de Panetta, un terrier color canela inseparable del entonces jefe de la CIA y futuro secretario de Estado de Defensa. “Quien quiera un amigo en Washington, que se compre un perro”, dejó dicho Truman, el presidente norteamericano (1945-1953) que precisamente creó la CIA. No se sabe si era por esta recomendación, pero Bravo estuvo presente en todas las reuniones de crisis a las que asistió Panetta. También en aquella en la que, meses más tarde, se seguiría en directo la muerte a Osama bin Laden.

Panetta bromea con el presidente para romper el hielo y le comunica que el virus “se ha extendido”. Fuera de la Casa Blanca, con menos información de la que se contaba en aquella reunión, expertos y medios de comunicación intentan explicar lo que está ocurriendo. Uno de los primeros reportajes publicados fue el de la periodista especializada en seguridad informática Kim Zetter, en la revista Wired. Desde entonces, Zetter ha continuado cubriendo la evolución de la trama e indagando en sus implicaciones. El resultado de todo ese trabajo está reunido en el libro dedicado al caso que publicaría hace ahora dos años (Zetter, 2014a).

Cuando tuvo noticia del malware a través del blog de Krebs, le llamó la atención que el objetivo del virus, uno de tantos, fuesen los sistemas SCADA. Era un tema que conocía bien porque ya había escrito sobre él, por la creciente dependencia de las infraestructuras críticas de este tipo de sistemas. A principios de aquel año, Zetter (2010d) había publicado, también en Wired, un extenso reportaje sobre el tema, en el que recogía los resultados de una encuesta realizada por la empresa de antivirus MacAffe que se estaba presentando en el Foro de Davos. Entre las más serias conclusiones del informe se encontraba la afirmación de que algunas de las infraestructuras críticas más sensibles de todo el mundo, como las de las industrias de energía y de recursos naturales (como el agua y

depuradoras de agua), eran también las menos seguras. El estudio recogía opiniones de los ejecutivos que trabajan para las entidades que utilizan SCADA (control, supervisión y adquisición de datos) o sistemas de control industriales. El 80 por ciento admitía que sus sistemas están conectados a Internet o a alguna otra red IP (con el riesgo de intrusión que esto supone). Alrededor del 55 por ciento de los encuestados en los sectores del petróleo, gas y electricidad informaban que los sistemas operativos de control SCADA eran con frecuencia objeto de ataques informáticos, aunque la encuesta no ofrecía ninguna indicación sobre su éxito. Además, solo el 57 por ciento de los encuestados en todos los sectores aseguraba que en su empresa se instalaban los parches de seguridad y actualizaciones de software de forma regular.

Otro reportaje anterior, también de Wired, había alertado hacía unos años sobre los fallos de estos sistemas a raíz de un accidente en un oleoducto en el Estado de Washington que acabó con la muerte de tres personas e hirió a otras ocho. Aunque el dramático suceso se debió a un cúmulo de circunstancias (errores humanos y daño accidental de las instalaciones por unas obras), también puso sobre la mesa la cuestión de la seguridad de los sistemas automatizados de control (Ryan, 2012). Entre los factores que coincidieron, se produjo uno que tardó tiempo en explicarse: un fallo informático que paralizó la sala de control central de operaciones y que comenzó 30 minutos antes del accidente, impidiendo que los trabajadores liberaran presión de la canalización. En aquel reportaje de Wired se recordaba:

Los expertos en seguridad y los investigadores del Gobierno han advertido desde hace tiempo que las complejas redes que controlan las infraestructuras críticas, como la red eléctrica y las tuberías de gas y petróleo, no fueron construidos pensando en la seguridad. En enero de 2003, el gusano Slammer penetró en un equipo de la red privada de la central nuclear Davis-Besse, de Ohio, y desactivó un sistema de monitoreo de seguridad durante casi cinco horas. Más tarde ese año, un error de software en un sistema de gestión de la energía de General Electric había contribuido a un corte de energía en cascada que dejó sin suministro eléctrico a 50 millones de

personas en ocho Estados y una provincia canadiense.

Por eso, cuando Kim Zetter conoce la existencia del virus descubierto por los bielorrusos, profundiza en la seguridad de los sistemas SCADA. La periodista destaca que el malware se dirige contra el software de control instalado en infraestructuras críticas y que utiliza una contraseña por defecto que el fabricante de software establece de forma fija en su sistema y que ya era conocida. La contraseña había estado disponible online al menos desde 2008, cuando se publicó en foros de productos en Alemania y Rusia. La contraseña protege la base de datos utilizada en el sistema Simatic WinCC SCADA de Siemens, que se ejecuta en los sistemas operativos Windows. Todavía hoy, los sistemas de control automático utilizan las contraseñas por defecto para que los suministradores puedan acceder a los sistemas para labores de mantenimiento.

El análisis de Boldewin mostró que, una vez que Stuxnet se ponía en marcha, buscaba en el ordenador la presencia del software Simatic WinCC y luego aplicaba la contraseña codificada, 2WSXcder, para acceder a la base de datos del sistema de control. “Las contraseñas predeterminadas son y han sido una vulnerabilidad importante durante muchos años”, admitía un experto. Pero esto, más que una negligencia, hay que verlo como una falta de percepción de la necesidad. Los programadores estaban más preocupados por el funcionamiento sin fallos de las instalaciones que por un posible ataque, en el que nadie habría pensado hasta que apareció Stuxnet. Es ahí precisamente donde se producirían las críticas más serias contra el virus: haber mostrado un camino que luego cualquiera iba a poder seguir.

El virus por dentro

¿Cómo era en realidad Stuxnet "por dentro"? ¿Cómo actuaba? Meses de trabajo de ingeniería inversa (determinar a partir de su código qué lo hace funcionar y cómo fue fabricado) de las principales empresas de seguridad del mundo fueron produciendo sucesivas informaciones a través de las que se pudieron conocer las propiedades del virus.

Bruce Dang, el ingeniero de seguridad de software del Centro de Respuesta de Seguridad de Microsoft que dirigió el análisis en la compañía, sabía que "muchas otras personas estaban buscando, y era importante para ellos saber los detalles antes que el resto". El código que tenían era grande, cerca de 1 MB de información. "Se formó un equipo de 20 a 30 personas con experiencia en diversos componentes del sistema de Windows y rápidamente comenzaron a intercambiar mensajes de correo electrónico con sus impresiones. Mediante la explotación de una vulnerabilidad en la función de acceso directo de Windows, o archivos .lnk, el gusano ganaba la capacidad de ejecutar comandos en el equipo infectado, pero a nivel de usuario" (Borland, 2010).

Un acceso directo es un vínculo a un archivo o programa, representado por un icono. Si se hace doble clic en un acceso directo, se abre el archivo o el programa. Es un mecanismo que se suele utilizar para mantener los archivos que se usan con frecuencia en una única ubicación de fácil acceso, como una carpeta o el escritorio. Los accesos directos se implementan como archivos con la extensión .lnk.

Caso cerrado. Ellos pensaban que solucionando ese fallo de seguridad habían terminado. Para Microsoft, era muy urgente parchear esa vulnerabilidad de su sistema operativo: estaban recibiendo informes de un número considerable de infecciones y la vulnerabilidad resultaba ser extremadamente fácil de usar. No obstante, una investigación más detallada mostró que el gusano era

capaz de aumentar sus privilegios para ejecutar código y, luego, instalar un rootkit.

Pensaron en cómo solucionar el problema y cambiaron la forma en que el programador de tareas de Windows Vista utiliza los valores hash para verificar los archivos. Una vez implementado, esto bloquearía la escalada peligrosa de privilegios.

Sin embargo, tampoco entonces habían acabado. Observaron que un archivo .DLL en particular (los .DLL son archivos del sistema) se estaba cargando en forma sospechosa. Dang comenzó revisando el código línea por línea, pero, con más de 1.000, pronto se dio cuenta de que la táctica no iba a ser lo suficientemente rápida. Desde el departamento de gestión les estaban presionando para que llegaran a algún resultado. Dang sabía que estaba buscando algo, pero no tenía claro qué exactamente. Al día siguiente, el equipo identificó un fallo en la forma en que los sistemas Windows XP permiten cambiar la distribución del teclado del usuario, lo cual permitía al gusano obtener privilegios de administrador.

Pero había más. El equipo recibió la noticia de que la compañía de seguridad Kaspersky Lab había detectado un extraño tráfico de "llamada a procedimiento remoto" que se enviaba a través de una red (un tipo de comunicación que permite a un ordenador iniciar una actividad; por ejemplo, la impresión desde un dispositivo remoto). Entonces, Dang y su equipo prepararon una simulación para comprobarlo: "Crearon un mini-VPN (una red local), infectaron un ordenador y se fueron. Volvieron y encontraron que la minired se había infectado por completo". "¡Pero ¿cómo es posible?! —exclamó Dang—, esto es muy raro".

El fallo era un defecto en la cola de impresión, que permitía a las cuentas de invitados remotos escribir archivos ejecutables directamente en el disco. Un atacante que aprovechara esta vulnerabilidad podría ejecutar código arbitrario como el usuario que ha iniciado la sesión. Si un usuario inicia sesión con derechos de usuario administrativos, un atacante podría lograr el control completo del sistema afectado. De esta forma, un intruso podría instalar programas; ver, cambiar o eliminar datos o crear cuentas nuevas con todos los derechos de usuario. Es decir, los usuarios cuyas cuentas estuvieran configuradas con pocos derechos de

usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.

A partir de su lectura del código, Dang sacó varias conclusiones claras: fue escrito por, al menos, varias personas. Y los creadores habían tenido cuidado de asegurarse de que se ejecutaba a la perfección, con alto impacto y el 100 por cien de confiabilidad. Un objetivo que incluso los desarrolladores de software comercial no logran satisfacer a menudo. El tiempo total desde el descubrimiento hasta la corrección final fue de entre tres y cuatro días, con una dedicación de alrededor de 40 horas por persona (Borland, 2010).

En la principal convención hacker de aquel año, el Chaos Computer Club, Dang (2010) presentó todo aquel proceso de análisis. Como escribió Kim Zetter (2011c), "la historia de Stuxnet podría haber terminado ahí". Al fin y al cabo, el virus presentaba aspectos nunca vistos, pero, en otros, "parecía poco ambicioso en sus objetivos". Se sabía ya que había sido diseñado para atacar el software Simatic WinCC, el sistema de control industrial de Siemens utilizado en programas que impulsan motores, válvulas e interruptores en decenas de procesos. Y "aunque esto era nuevo era en sí mismo —los sistemas de control no son un objetivo de los piratas informáticos tradicionales, porque no hay ningún beneficio económico evidente—, lo que parecía que el virus hacía no resultaba tan innovador: daba la impresión de haber sido simplemente un robo de datos de configuración y diseño de los sistemas, presumiblemente para permitir que un competidor duplicase el diseño de producción de una fábrica. Parecía otro caso más de espionaje industrial", contaba Zetter.

Por aquel entonces, las compañías antivirus ya habían incorporado a sus motores de detección actualizaciones para neutralizar las distintas versiones del software malicioso y podían dedicar su atención a otras cosas. Pero, de nuevo, el desarrollo de los hechos iba a dar un giro. El responsable: Liam O'Murchu.

Este ingeniero de origen irlandés, que se define en su perfil de Twitter como "Investigador de seguridad y de técnicas de ingeniería inversa en Symantec, con más conocimiento de enriquecimiento de uranio y centrifugadoras del que me gustaría", fue el primero que se dio cuenta de que el virus era más complejo de lo que se creía hasta

entonces. O'Murchu es, por lo que cuenta la periodista Kim Zetter (2011c), un hacker de libro:

Su primer encuentro con el malware había sido en 1996, cuando un compañero de estudios en el colegio de Dublín creó un virus que atacó la red de la universidad. Cientos de terminales de los laboratorios de computación de la escuela quedaron bloqueados hasta que los estudiantes pudieran responder a 10 preguntas que destellaban en sus pantallas. La mayoría se irritaron por las molestias, pero O'Murchu estaba fascinado por el código y lo desarmó para ver cómo funcionaba. Era parte de su ADN, deconstruir las cosas. De pequeño había sido el tipo de niños que, en vez de jugar con un coche de juguete, lo destrozaba para descubrir cómo funcionaban los engranajes. La curiosidad fue lo que lo llevó a la seguridad informática.

Symantec, donde O'Murchu trabaja como responsable de seguridad, se encontraba entre las empresas que en julio habían capturado el código del virus para crear actualizaciones para sus productos anti-malware.

Según narra Zetter (2011c), "de más de un millón de archivos maliciosos que Symantec y otras firmas de antivirus reciben mensualmente, la mayoría son variaciones de los virus y gusanos ya conocidos. Estos se procesan de forma automática sin intervención humana. Algoritmos rastrean los archivos en busca de comportamientos o cadenas de datos reveladores para identificar el malware y, a continuación, producen actualizaciones para los escáneres antivirus en los equipos de los clientes". Pero los malware que contienen exploits de día cero son especiales y se examinan a mano, y así llegó a O'Murchu.

Cuenta Kim Zetter que el irlandés pasó Stuxnet a un ingeniero sin experiencia en días cero pensando que sería una buena oportunidad para entrenarlo. Pero mientras se metía en el código, se dio cuenta de que era mucho más complejo de lo que pensaba, "parecía demasiado sofisticado para un mero espionaje". Varias capas de

enmascaramiento oscurecían el exploit de día cero en el interior, y el malware era enorme: 500k bytes, en lugar de la habitual 10k a 15k. Lo más destacado, sin embargo, fue la forma en que el malware se ocultaba. El virus almacena su archivo .DLL malicioso descifrado solo en la memoria (y no en el disco, duro como se hubiese esperado) como un tipo de archivo virtual con un nombre especialmente diseñado.

En todos sus años de análisis de malware, O'Murchu nunca había visto una técnica parecida. Era "una nueva raza de archivo fantasma que no se almacenaba en el disco duro en absoluto y, por lo tanto, sería casi imposible de encontrar" Zetter (2011c). A O'Murchu se unieron Eric Chien, director técnico de Symantec Security Response, y Nicolas Falliere, un ingeniero de software y analista sénior de la oficina de Symantec en París.

Descubrieron que, cada vez que Stuxnet infectaba un sistema, "llamaba por teléfono a casa" a uno de los dos dominios (www.mypremierfutbol.com y www.todaysfutbol.com) alojados en servidores en Malasia y Dinamarca para reportar información de las máquinas infectadas. Esto incluía direcciones de la máquina interna y externa IP, el nombre del equipo, su sistema operativo y versión de software, y si el software de Siemens, Simatic WinCC Step7, también conocido como "Step7", se había instalado en la máquina. Los servidores de comando y control permitían a los atacantes actualizar Stuxnet en las máquinas infectadas con nuevas funcionalidades, e incluso instalar más archivos maliciosos en los sistemas. Los proveedores de DNS para los dos dominios ya habían eliminado el tráfico entrante para evitar que llegase a los atacantes. Pero Symantec tuvo una idea mejor: convencer a los proveedores de que redirigieran el tráfico a un equipo controlado por Symantec (Zetter, 2011c).

A los pocos días, Symantec estaba recibiendo informes de las máquinas que Stuxnet había infectado. Una semana después, recibían informes de unos 38.000 equipos infectados desde decenas de países. En poco tiempo, el número sobrepasaría los 100.000. Stuxnet se había extendido rápidamente, a pesar de las actualizaciones distribuidas por las firmas antivirus para detectarlo y neutralizarlo.

Como Chien y O'Murchu habían asignado una ubicación geográfica a las infecciones, descubrieron un extraño patrón: de las 38.000 infecciones iniciales, unas 22.000 estaban en Irán. Indonesia estaba en un distante segundo lugar, con cerca de 6.700 infecciones, seguida por India, con cerca de 3.700 infecciones.

El 16 de julio hicieron público su primer análisis sobre el virus, dando a conocer los países donde se estaban produciendo más infecciones y cómo Stuxnet se aprovechaba de la contraseña por defecto para acceder a la base de datos del sistema SCADA. En su informe, lo explicaban así: "Los archivos .lnk son parte de la explotación y se utilizan para cargar dos archivos temporales. La amenaza contiene muchas funciones diferentes. Nuestro análisis sobre ellas está actualmente en curso. Sin embargo, podemos afirmar en este momento que la amenaza está utilizando algunos archivos DLL de Siemens del producto Step7 para acceder a los sistemas SCADA. Se utiliza un nombre de usuario y la contraseña predeterminada para conectarse a la base de datos asociada con el SCADA" (Symantec, 2010a).

Un año después, en un reportaje para Wired con motivo del primer aniversario del descubrimiento del virus, Kim Zetter (2011c) preguntó a los ingenieros de Symantec si, en ese momento, se encontraron en un conflicto de intereses. Eric Chien, director técnico de Symantec Security, respondió: "Para nosotros, no hay buenos ni malos. Bueno, chicos malos son gente que está escribiendo código malicioso que infecta los sistemas que pueden causar consecuencias no deseadas o consecuencias deseadas. Si el "malo" fue Estados Unidos o uno de sus aliados, el ataque estaba causando daños colaterales a miles de sistemas, y Symantec no sentía ningún deber patriótico de preservar su actividad. Somos una empresa multinacional privada que protege a sus clientes".

Symantec continuó sus investigaciones y el 14 de septiembre sacó a la luz un nuevo bombazo: Stuxnet no se aprovechaba solo de una vulnerabilidad día cero, sino de cuatro. Liam O'Murchu (2010b) publicó en el blog de la compañía antivirus un artículo dándolo a conocer:

Stuxnet está utilizando tres vulnerabilidades adicionales de día cero. Una amenaza [informática] que utiliza una vulnerabilidad de día cero es por sí misma todo un acontecimiento. Sin embargo, una amenaza a través de cuatro vulnerabilidades de día cero es extraordinaria y única. Esta es la primera vez que encuentro una amenaza que utiliza tantas vulnerabilidades desconocidas y sin parches. No solo Stuxnet hace uso de vulnerabilidades de día cero, sino que también utiliza una variedad de otras (como la vulnerabilidad de Microsoft Windows Server Service RPC, que permite la ejecución remota de código), lo que demuestra la extraordinaria sofisticación, el pensamiento y la planificación que intervinieron en la fabricación Stuxnet.

Como explica Zetter (2010a), un día cero se utilizaba para propagar el gusano a una máquina mediante una memoria USB. Una vulnerabilidad en la cola de impresión de Windows para propagar el malware de una máquina infectada a otras personas en una red. Los dos últimos ayudaban al malware a obtener privilegios administrativos en las máquinas infectadas para poder ejecutar comandos del sistema.

Además de las vulnerabilidades día cero, al estar firmado digitalmente con certificados legítimos robados de dos autoridades de certificación, y los sistemas de ocultación que incorporaba, el atacante utilizaba una vulnerabilidad en el servicio RPC de ejecución remota (una funcionabilidad de Windows) para actualizar el código en las máquinas infectadas y, también, en caso de que el servidor estuviera caído, redes P2P (peer-to-peer) para propagar cambios a las máquinas infectadas.

El hombre que descubrió que Stuxnet era un arma

Había una persona especialmente pendiente de los informes que Symantec iba publicando sobre Stuxnet, Ralph Langner, un ingeniero alemán especializado en la programación de sistemas SCADA. Symantec había profundizado en cómo explotaba el malware las vulnerabilidades de Windows, y sus modos de propagación, pero carecían de conocimientos suficientes sobre los sistemas de control automatizado para determinar el objetivo final de tanta sofisticación en el código de un virus.

El 16 de septiembre, Langner (2010e) publica en el blog de su compañía un artículo que remataba con un rotundo: “Bienvenidos a la ciberguerra”. Langner fue la primera persona que estableció que Stuxnet había sido creado para el sabotaje y no era un malware de espionaje más: “Stuxnet tiene la precisión, a nivel cibernético, de un misil desplegado para buscar y destruir un objetivo en el mundo real de gran importancia. Un objetivo que aún se desconoce”, afirmaba el ingeniero alemán, y proseguía: “Stuxnet es un ataque cibernético destinado al 100 por cien a destruir un proceso industrial en el mundo físico. No se trata de espionaje, como algunos han dicho. Se trata de un sabotaje 100 por cien”.

Una semana después, Langner publica un nuevo análisis. Para él, Stuxnet era una pieza de una operación por etapas: “Muchos aspectos de Stuxnet son tan completamente diferentes del software malicioso que conocemos que es natural que, en algún momento, el análisis de tantos expertos que trabajan duro termine en frustración”, decía. “La mejor manera de acercarse a Stuxnet es no pensar en él como una pieza de malware, sino como parte de una operación”, que él denominó “Myrtus”.

En realidad, Langner solo dejó de acertar en una cosa: la operación ya estaba en marcha, pero con otro nombre en clave: “Juegos Olímpicos”. Según deducía el alemán, las etapas de esa operación habrían sido cuatro:

Etapa 1. La preparación, que habría incluido la formación de un equipo de varias unidades; el montaje del desarrollo y el laboratorio de pruebas, incluyendo el modelo de proceso; la planificación de aspectos del destino, incluyendo la identificación de las personas clave para la infiltración inicial del virus y el robo de certificados digitales.

Etapa 2. La infiltración, que habría comprendido las siguientes acciones: infiltración, utilizando memorias USB iniciales; el arma [Stuxnet] se extiende localmente a través de intercambio de memoria USB, carpetas compartidas, colas de la impresora; contacto para comandar y controlar los servidores y tener evidencia de que están comprometidos; actualización mediante redes P2P; apagado de los servidores.

Etapa 3. Ejecución. Etapa final en la que habría debido comprobar la configuración del controlador PLC; identificar los controladores individuales que iban a ser el objetivo del ataque; cargar la "reprogramación" del controlador; ocultar esta "reprogramación" a los ingenieros del sistema de control; comprobar el estado del proceso y, por último, activar la secuencia de ataque.

Para Langner, esto demostraría que "los exploits día cero fueron solo de uso temporal durante la fase de infiltración. ¡Todo un lujo para tales hazañas!", dijo. "Después de que el arma esté en su lugar, el ataque principal se ejecuta en los controladores", añadió. A lo que llamó "ingeniería de ataque".

Ese mismo día, Symantec, una vez que Langner les había puesto sobre la pista, publicaba un artículo en el que explica el proceso por el que Stuxnet tomaba el control de un sistema SCADA (Falliere, 2010). Explican que el objetivo de Stuxnet es modificar el comportamiento de un sistema de control industrial mediante la modificación de los PLC [autómatas programables]. Esto lo hace en varios pasos sucesivos: la interceptación de peticiones de lectura-escritura enviados al PLC; la determinación de si el sistema es el objetivo previsto; la modificación de los bloques de código PLC

existentes y la escritura de nuevos bloques al PLC. Finalmente, oculta la infección al PLC usando funcionalidad de rootkit. Para las distintas tareas se habían usado lenguajes de programación diferentes: por ejemplo, la ocultación de los bloques de código infectados se llevaba a cabo en la máquina usando C / C + +, mientras que el código malicioso que Stuxnet pretende ejecutar en el sistema de control industrial está escrito en el lenguaje ensamblador que se ejecuta en los PLC. Es decir, que el "malware habría requerido un equipo o equipos de personas con capacidades diferentes —algunas de ellas con un amplio conocimiento del PLC objetivo y otras que se especializan en el estudio de vulnerabilidades para encontrar los agujeros de día cero, según los analistas—. El malware habría requerido pruebas exhaustivas para garantizar que podría comandar un PLC sin que se caiga el sistema o de salir otras alertas de su presencia" (2010a).

Pero aún faltaba un dato esencial por desentrañar: ¿qué hacía Stuxnet una vez que tenía el dominio sobre los autómatas programables? ¿Cómo los modificaba en concreto y con qué finalidad?

Así saboteó Stuxnet la planta nuclear de Natanz

El 15 de noviembre de 2010, Symantec (2010b) publica un extenso dosier sobre Stuxnet, que recoge toda su investigación hasta el momento. Entre los datos nuevos se incluye el descubrimiento de qué función en concreto del sistema SCADA es modificada por el virus: Stuxnet estaba diseñado para provocar una alteración de frecuencias. Habían descubierto, además, que el malware se dirigía específicamente a los sistemas de Siemens que se utilizan con unidades de convertidores de frecuencia realizadas por dos empresas, una basada en Irán y otra en Finlandia.

Y, aún más específicamente, los objetivos de Stuxnet eran solo variadores de frecuencia de estas dos empresas que se ejecutan a altas velocidades —entre 807 Hz y 1210 Hz—. Estas unidades se encuentran en fuentes de alimentación utilizadas para controlar la velocidad de un dispositivo, como un motor.

Stuxnet interceptaba los comandos enviados a las unidades desde el software SCADA de Siemens y los reemplazaba con comandos maliciosos para controlar la velocidad de un dispositivo, que variaban salvajemente, pero de forma intermitente. Todos los datos indicaban que los creadores del malware "tenían una instalación o instalaciones específicas en mente para el ataque, y un amplio conocimiento del sistema contra el que se dirigían" (Zetter, 2010a). Y no solo eso. También debía suponerse que los atacantes habían tenido oportunidad de probar, en un entorno simulado, que Stuxnet funcionaría según lo previsto, logrando los resultados esperados.

Un aspecto llamativo era el largo tiempo de espera que pasaba entre las diferentes etapas de los procesos maliciosos iniciados por el código, en algunos casos más de tres semanas. Para los técnicos de Symantec, esto indicaba que los atacantes estaban interesados en quedarse allí sin ser detectados, en lugar de pretender un sabotaje rápido que pudiera ponerles sobre aviso. Stuxnet fue diseñado para ocultarse de ser detectado incluso si los administradores de una

instalación específica se dieran cuenta de que algo en el proceso había cambiado. Esto probablemente hubiese seguido así, en secreto y sin ser detectado, si Stuxnet no llega a salir a la luz tras el descubrimiento de Sergey Ulasen.

La relación de Stuxnet con Irán y, en particular, con algunas de sus instalaciones nucleares, era una especulación que siempre estaba presente en las noticias sobre el virus desde que Frank Boldewin apuntó en el foro de wildersecurity.com que el objetivo del virus era un sistema SCADA y se supo las zonas donde se habían producido más infecciones (Zetter, 2010a y 2010e).

Sin embargo, durante los primeros meses, la hipótesis era que más bien se trataba de una operación de ciberespionaje. Hasta que los descubrimientos de Symantec sobre la "misión" del virus que revelaba el análisis de su código y los conocimientos de Langner sobre la programación y funcionamiento de los sistemas SCADA habían permitido unir piezas y establecer la tesis del sabotaje.

Pero ¿dónde y con qué efectos? Aún faltaba una pieza en el puzle: las consecuencias de Stuxnet en una instalación concreta. "Un arma de un solo tiro", así había definido Ralph Langner a Stuxnet tras haber establecido que se trataba de un "ciberarma" y no solo de un software espía. Langner aventuraba que, probablemente, ese ataque ya se habría producido.

El cuadro se iba a completar con las revelaciones de David Albright, del Instituto para la Ciencia y la Seguridad Internacional. Después de leer los informes de Langner y el equipo de Symantec, Albright reveló en diciembre que la frecuencia nominal a la que operaban centrifugadoras de Natanz es de 1,064Hz, justo la frecuencia exacta que Stuxnet restaura en los convertidores después de haberla aumentado y disminuido drásticamente durante el ataque del software malintencionado. Albright encontró otra correlación: los datos de Stuxnet indicaban que estaba dirigido para atacar dispositivos configurados en grupos de 164; Albright señaló que cada una de las cascadas de Natanz tenían 164 centrifugadoras. El misterio del destino de Stuxnet, y de las centrifugadoras dañadas [meses atrás se había producido un descenso en el número de las que estaban operativas, cuya causa nadie conocía], parecía estar resuelto (Zetter, 2011a).

¿Qué es una cascada? Las centrifugadoras de gas utilizadas para el enriquecimiento de uranio se reúnen en grupos para maximizar la eficiencia. Hasta 2012, Irán utilizaba cascadas con 164 centrifugadoras agrupadas en 15 etapas, con la etapa 10 como la etapa de alimentación (Langner, 2013). A partir de ahí, los datos sobre los fallos y anomalías que se estaban produciendo en la planta, y que llevaban observándose desde hacía tiempo, empiezan a cobrar sentido. Los efectos más visibles de Stuxnet se habrían registrado meses antes, cuando comenzaron a girar centrifugadoras más rápido de lo normal, a velocidades que habían hecho que los componentes sensibles comenzaran a deformarse y romperse.

Los inspectores de la agencia encargados de revisar, por mandato de las Naciones Unidas, la actividad de Natanz, habían detectado una inusual renovación de centrifugadoras entre noviembre de 2009 y febrero de 2010: si normalmente se reemplazaban en un año el 10 por ciento de las mismas por razones de mantenimiento, en esa ocasión se habían llegado a sustituir más de 1.000 centrifugadoras IR-1 (Albright, Brannan y Walrond, 2010). Las estadísticas recogidas unos meses antes, a finales de 2009, por la Agencia Internacional de Energía Atómica (AIEA) muestran un descenso brusco en el número de centrifugadoras de enriquecimiento entre junio y noviembre de aquel año, pasando de 4.920 a 3.936 (las IP-1); y de 45 a 13 (las IR-2/3/4). Pero entonces no se sospechaban las causas y el propio Gobierno de Irán estaba igual de desconcertado. Ahora ya podían atribuirse estos desperfectos a Stuxnet.

Finalmente, el 23 de noviembre de 2010, la AIEA publica un informe dando a conocer que las instalaciones de la planta de Natanz de producción de combustible para enriquecimiento de Uranio estaban temporalmente suspendidas (Crawford y Solomon, 2010). Tras este informe de la AIEA (2010), el Gobierno de Irán reconoce, unos días después, que aceleradores de su planta de Natanz (sin nombrarla) se habrían visto dañados por un malware que afectaba a los procesos y provocaba desperfectos en las instalaciones de planta obligando a su sustitución (Zetter, 2010c).

El 7 de diciembre, Siemens informó que había descubierto 417 códigos de ataque en sus autómatas programables (Langner,

2010d). El virus había cumplido, aparentemente, su misión de demorar el plan nuclear iraní, aunque todavía hoy no hay acuerdo sobre el balance real del ataque.

Sin embargo, aún había daños previos que no estaban claros todavía. En julio de aquel año (2009), el presidente Ahmadinejad había aceptado la dimisión del jefe del programa nuclear de Irán, Gholam Reza Aghazadeh. Entonces se especuló con posibles motivos políticos, pero al día siguiente WikiLeaks publicó una nota informativa, firmada por Julian Assange, en la que dejaba ver que un "serio accidente nuclear" podía estar detrás de la dimisión de Aghazadeh (WikiLeaks, 2009).

Según la AIEA, el número de cascadas que estaban siendo alimentadas con gas y la cantidad de gas empleado comenzó a caer en algún momento entre enero y agosto de 2009 (Zetter, 2013b), periodos en los que el virus aún no estaba en Natanz. Luego se supo que estos fallos se debían a una versión anterior de Stuxnet (Stuxnet 0.5, descubierta por Liam O'Murchu, de Symantec) que afectaba, no a la velocidad de las centrifugadoras, sino a las válvulas de presión (Symantec, 2013; Zetter, 2013b).

Esta versión, aún más furtiva, incluía una funcionalidad "que parecía de película": el programa grababa secretamente el funcionamiento normal de los controladores de la planta; cuando los operadores los chequeaban en busca del motivo de las incidencias, Stuxnet "mostraba" esa secuencia, "como en los robos de los bancos cuando los atracadores engañan a las cámaras de seguridad mostrándoles un vídeo pregrabado" (Broad, Markoff y Sanger, 2010). Es decir, que los daños a instalaciones de la central de Natanz se habían producido en dos momentos, por dos versiones de Stuxnet distintas, atacando cada una de ellas a una parte del sistema.

En 2007, una persona no identificada había publicado una muestra de código en la plataforma colaborativa del antivirus Virustotal, que más tarde resultó ser la primera variante de Stuxnet conocida (Stuxnet 0.5). Aunque no fue advertido por ninguna compañía antivirus en el momento, el código contenía una carga útil para interferir severamente en el sistema de protección en cascada (CPS) en la planta de enriquecimiento de Natanz (Langner, 2013).

El ataque de Stuxnet 0.5 se dirigió contra el sistema de protección de la cascada, infectando a los controladores de Siemens S7-417, un controlador industrial para tareas de automatización grandes. En Natanz se utilizaba para controlar las válvulas y sensores de presión de hasta seis cascadas (o 984 centrifugadoras). Inmediatamente después de la infección de la carga útil de esta variante temprana, Stuxnet asumió el control completo de los controladores de Siemens.

Los sistemas de protección no sirven a ningún propósito durante el funcionamiento normal de la instalación, pero están destinadas a detectar anomalías en el proceso y evitar que la destrucción de los equipos se convierta en un peligro para los operadores y el medio ambiente. Stuxnet 0.5 afectaba al funcionamiento de las válvulas que controlan el flujo de gas de hexafluoruro de uranio en las centrifugadoras y cascadas. El objetivo del malware era manipular el movimiento de gas de tal manera que la presión dentro de las centrifugadoras y la cascada aumentase cinco veces la presión de funcionamiento normal. Stuxnet 0.5 cerraba las válvulas de 6 de cada 18 cascadas y modificaba otras en centrifugadoras individuales elegidas al azar para evitar que los operadores detectasen un patrón de problemas.

El siguiente ataque se produjo con la nueva variante de Stuxnet, descubierta en junio de 2010 por Sergey Ulasen, que atacaba a un componente completamente diferente: el sistema que regula la velocidad del rotor y que está controlado por un dispositivo también diferente al del primer ataque, el controlador S7-315 de Siemens.

Tal como estaba programado el virus, y tal como funcionó, el plan era más provocar el deterioro de piezas vitales mediante un funcionamiento extremo (a más presión o velocidad de la adecuada) de forma prolongada e intermitente que “de un solo golpe”, que hubiese favorecido una detección más automática del sabotaje.

Años más tarde, en 2013, Ralph Langner publicará un detallado estudio donde explica estos detalles y pormenoriza los daños “físicos” de Stuxnet en las instalaciones de Natanz a partir de la “reprogramación” de los autómatas del sistema. El título: Matar a una centrifugadora… (Langner, 2013). En él aclara algunos aspectos

que, o no estaban claros, o no se habían transmitido adecuadamente a través de la mayoría de los medios de comunicación que habían informado del caso.

Langner destaca la importancia de comprender el modelo de ataque "en tres capas" que Stuxnet había supuesto para prevenirlos adecuadamente en el futuro: a diferencia de los ataques cibernéticos habituales, un ataque cibernético físico como el de Stuxnet implica tres capas y sus vulnerabilidades específicas: la capa TI (tecnología de la información), que se utiliza para propagar el malware; la capa del sistema de control, que se utiliza para manipular (pero no interrumpir) el proceso control y, finalmente, la capa física, donde se crea el daño real.

En el caso del ataque cibernético contra Natanz, la vulnerabilidad en la capa física fue la fragilidad de los rotores de centrifugadoras, que explotaron por las manipulaciones de la presión del proceso (en el primer ataque de Stuxnet 0.5) y la velocidad del rotor (en el segundo ataque, el de la versión de Stuxnet descubierta por Sergey Ulasen). "El malware Stuxnet lo convierte en un ejemplo de manual de cómo la interacción de estas capas se puede aprovechar para crear destrucción física por un ataque cibernético", dice Langner.

‘Un tipo de amenaza que esperamos no volver a ver nunca’

Si alguien duda del alcance de Stuxnet como primer ciberarma, más allá de los daños físicos concretos que logró causar en Natanz, es recomendable que lea el sumario del informe de Symantec (2010b), donde presentaban sus conclusiones tras meses de análisis del virus:

Stuxnet representa el primero de muchos hitos en la historia de código malicioso —que es el primero en explotar cuatro vulnerabilidades “día cero”, se usan dos certificados digitales robados, se inyecta código en los sistemas de control industrial y ocultan el código al operador—. Queda por ver si Stuxnet es el comienzo de una nueva generación de ataques de código malicioso hacia infraestructuras del mundo real o si se trata de una contingencia que se da una vez por década.

Stuxnet es de tal complejidad —requiriendo recursos significativos para poder desarrollarlo— que pocos atacantes serán capaces de producir una amenaza similar, hasta el punto de que no esperaríamos que amenazas en masa de sofisticación similar aparezcan de repente.

Sin embargo, Stuxnet ha puesto de manifiesto que los intentos de ataque directo a infraestructuras críticas son posibles, y no solo en la teoría o en la trama de películas.

Las implicaciones de Stuxnet en el mundo real están más allá de cualquier amenaza que hayamos visto en el pasado. A pesar del

desafío emocionante de ingeniería inversa y de comprensión de su propósito que ha supuesto, Stuxnet es el tipo de amenaza que esperamos no volver a ver nunca.

El 6 de octubre de 2010, cuando el virus está en proceso de descubrimiento, en un post en el que se queja de las carencias de los medios de comunicación explicando las implicaciones de Stuxnet, Ralph Langner (2010e) concluye:

Esa es la verdadera amenaza que Stuxnet plantea para todos nosotros: proporciona un modelo para los ataques agresivos en los sistemas de control que se pueden aplicar de forma genérica. Dependiendo de dónde vivas, tales sistemas de control pueden controlar la planta de energía que proporciona tu energía eléctrica, la empresa de canalización que proporciona tu agua, la fábrica en la que trabajas y el semáforo que ves en tu camino a casa. La tecnología para manipular todos estos sistemas está ahora en la calle, y no seas tan ingenuo como para suponer que nadie se aprovechará de ella. Por desgracia, los CERT y organizaciones similares no tienen las agallas para decirte esto, a pesar de que es su obligación y de que están pagados con dinero de los contribuyentes. Sin embargo, ahora ya lo sabes.

Los pacientes cero

Del caso Stuxnet hubo un dato que tardó años en salir a la luz: quiénes habían sido los "pacientes cero", es decir, los primeros infectados por los virus para ser intermediarios en el camino del malware hasta Natanz. En 2011, en la actualización de su dosier sobre Stuxnet, Symantec precisó cómo se habían producido estas infecciones en tres olas. La primera, contra cuatro "blancos", se inició el 23 de junio de 2009 a las 4.40.16 horas. La segunda, contra uno de esos objetivos, el 23 de marzo de 2010 a las 6.06.07 horas. La tercera ola incorporó un blanco más y comenzó el 26 de abril de 2010. Sin embargo, no se llegó a identificar a las empresas que en concreto habían sido atacadas.

Fue Kaspersky quien las identificó a través de un informe al que tituló "Stuxnet: víctimas cero. La identidad de las compañías apuntadas por el primer ciberarma conocida" (Kaspersky Lab, 2014) y que publicó en noviembre de 2014. Según la empresa de seguridad rusa, las cuatro organizaciones que fueron atacadas inicialmente estaban trabajando en el entorno de una compañía iraní de telecomunicaciones que se dedica a la instalación, suministro, diseño, programación y mantenimiento de sistemas SCADA, estaciones de monitorización y redes de telecomunicaciones (Iran Control and Communication System Supply Co.) o en el suministro de materiales y piezas para este tipo de sistemas. La quinta organización atacada, entre otros productos para la automatización industrial que fabrica, produce centrifugadoras de enriquecimiento de uranio. Este es precisamente el tipo de equipo que habría sido el principal objetivo de Stuxnet.

Los atacantes esperaban que estas organizaciones intercambiaran datos con sus clientes —la planta de enriquecimiento de uranio— y, de esta manera, conseguir introducir el malware en las instalaciones de destino. "El análisis de la actividad profesional de las primeras organizaciones que son víctimas de Stuxnet nos da una mejor

comprensión de cómo se planeó toda la operación. En definitiva, este es un ejemplo de un vector de ataque a la cadena de suministro, donde el malware se hace llegar a la instalación destino indirectamente a través de redes de socios con los que es posible que trabaje", afirmaba Alexander Gostev, experto jefe de seguridad de Kaspersky Lab.

Además, los expertos de Kaspersky hicieron otro descubrimiento interesante: el gusano Stuxnet no solo se extendió a través de USB infectados conectados al PC, según la escasa diferencia temporal entre que un atacante compiló la muestra, lo puso en un lápiz de memoria USB y lo entregó a la organización de destino. "Es razonable suponer que, en este caso particular, la gente detrás de Stuxnet utilizó otras técnicas en lugar de una infección USB", dijeron. Pero ¿quiénes eran realmente los que estaban detrás de Stuxnet?

La orden de crear Stuxnet, la primera arma cibernética

Los datos que arrojaba el virus sobre sí mismo dejaban claro que detrás de su desarrollo se encontraba una gran organización, con importantes recursos, con una cierta sensación de impunidad (como demostraba el robo de los certificados digitales, probablemente mediante el acceso físico a las oficinas de las certificadoras, dada su cercanía) y con posibilidades de probar in situ el funcionamiento del virus sobre un sistema SCADA.

Si a estos indicios se añadía el factor de la motivación, todas las miradas apuntaban a Estados Unidos o Israel. Sin embargo, durante dos años, no hubo pruebas para confirmar, más allá de la conjetura, esta tesis. Sin embargo, esto cambiaría en junio de 2012, cuando The New York Times publica un reportaje en el que por primera vez se narra la reunión de crisis que había tenido lugar en la Casa Blanca cuando el virus empezó a ser conocido y que ratifica la implicación de ambos Estados a partir de testimonios de algunos de los asistentes. El reportaje confirma por primera vez que Stuxnet había sido creado por la NSA con ayuda de Israel.

La Operación Juegos Olímpicos había sido desarrollada durante la Administración de George W. Bush. Obama fue informado por primera vez del programa incluso antes de asumir el cargo. El presidente saliente le había puesto al tanto de los pormenores de la estrategia iniciada años atrás y le instaba a seguir adelante con ella. El objetivo —según los testimonios del Gobierno que recogió The New York Times— era dañar la capacidad nuclear de Irán gradualmente y a la vez sembrar la confusión entre los científicos iraníes acerca de la causa de los contratiempos. Se suponía que la ciberarma haría pensar a los iraníes que sus ingenieros eran incapaces de ejecutar una instalación de enriquecimiento. Según la versión que miembros de la operación transmitieron al periódico neoyorkino, la idea era que los errores se dilatasen el mayor tiempo posible, en lugar de un ataque de un solo golpe. De hecho, fue así:

esa estrategia acabaría siendo deducida por los informáticos que analizaron Stuxnet a partir del análisis de su código y su forma de funcionar. “Si fuera una destrucción inmediata, total, por lo general, podrían averiguar lo que pasó y no se parecería a la incompetencia”, pensaron en la NSA al idear la operación, según declararon a The New York Times testigos de esas reuniones. Asimismo, esas fuentes del Gobierno confirmaron, tal como se sospechaba, que Stuxnet había llevado meses de pruebas y desarrollo.

Algunas informaciones apuntaban al general Cartwright como estratega de la operación. Sin embargo, “el trabajo pesado” fue hecho por la director de la NSA, Keith Alexander, que tenía “‘el know-how’ técnico y fue quien llevó a cabo la actividad real”, declaró a The Washington Post, quien rastreó la noticia tras la exclusiva del The New York Times, un exfuncionario anónimo (Nakashima, y Warrick, 2012).

En 2013, Cartwright sería procesado (Yoste, 2013) por haber sido la supuesta fuente de las filtraciones sobre el papel del Gobierno en la creación de Stuxnet, aunque finalmente terminarían por levantarse los cargos, con el argumento de que su enjuiciamiento supondría desclasificar documentos secretos (Scarborough, 2015).

En la fase de pruebas de Stuxnet jugó un papel esencial el complejo de Dimona, en el desierto de Negev, famoso como el corazón del fuertemente custodiado programa israelí —no reconocido— de armas nucleares. Durante dos años, Dimona habría asumido un papel secreto como banco de pruebas de Stuxnet. Allí, Israel hizo girar centrifugadoras nucleares, prácticamente idénticas a las de Natanz, comprobando la efectividad del virus (Broad, Markoff y Sanger, 2010). “Para probar el gusano, hay que conocer las máquinas”, dijo a The New York Times un experto estadounidense en inteligencia nuclear. “La razón por la que ha sido efectivo es porque los israelíes llevaron eso a cabo” (ibídem).

En aquel comité de crisis en la Situation Room del sótano del ala Oeste de la Casa Blanca, el núcleo duro de la Operación Juegos Olímpicos informa a Obama y al vicepresidente Biden de la situación, una vez que Stuxnet es ya de conocimiento público: un error en el código —explicaron a Obama— había llevado a extenderse al ordenador de un ingeniero cuando estaba conectado a

las centrifugadoras (Sanger, 2012). Según la versión que transmiten a The New York Times, le explican al presidente que cuando un ingeniero salió de la planta de Natanz y conectó su ordenador a Internet, “el virus, por un fallo de programación, no habría reconocido que su entorno había cambiado y habría comenzado replicarse a sí mismo en equipos de todo el mundo”. Según este relato, la cúpula de seguridad habría atribuido la responsabilidad del supuesto “escape” a Israel, que también formaba parte activa en la Operación Juegos Olímpicos. “Creemos que hubo una modificación hecha por los israelíes”, le habrían dicho al presidente, según recogió el diario neoyorkino, “fueron demasiado lejos”.

En realidad, tal como se comprobó tiempo después, este razonamiento no era sostenible. Según Symantec (O’Murchu, 2014; Kaspersky Lab, 2014), fue justo al contrario: Stuxnet infectó Natanz después de haberlo hecho a empresas que suministraban materiales y equipos a la planta. Además, técnicamente era imposible la propagación dentro-fuera por el propio funcionamiento del virus una vez que atacaba los autómatas, tal como señaló Langner en su informe sobre los daños de Stuxnet al sistema SCADA de Natanz (Langner, 2013).

Cuando el virus “se expandió” (en realidad, cuando fue de conocimiento público), Obama preguntó en aquella reunión por los riesgos; quería saber si el resto de la Operación Juegos Olímpicos estaba en peligro, “ahora que una variante del virus se replicaba a sí mismo en estado salvaje, cuando expertos en seguridad informática podían diseccionar y averiguar su propósito”. “No creo que tengamos suficiente información”, dijo Obama al grupo ese día, según transmitieron a The New York Times los funcionarios presentes.

El recién electo presidente se habría preocupado por los efectos contraproducentes del uso de la ciberarma. De hecho, “la infraestructura de ningún país es más dependiente de los sistemas informáticos y, por lo tanto, más vulnerable a los ataques que la de Estados Unidos. Es solo una cuestión de tiempo que sea objetivo de la misma clase de arma que los americanos han utilizado, en secreto, contra Irán” (Sanger, 2012). Sin embargo, habría ordenado

—según el relato filtrado— que los ataques cibernéticos continuaran. —Una afirmación que también se va a poner en duda más tarde, pues, según la configuración del virus, una eventual "cancelación" no era posible ni tenía sentido una vez que ya se había logrado la reprogramación de los autómatas (Langner, 2013) —.

Años después se sabría, por una exclusiva de The Intercept a partir de uno de los documentos de Snowden, que la NSA asumía que Irán habría aprendido las técnicas de los ciberataques de los que había sido objeto (con Stuxnet y otros tres virus relacionados: Duqu, Wiper y Flame) y que estaría en condiciones de usarlas contra objetivos occidentales (Greenwald, 2015).

La aparición de Stuxnet y la intrusión informática en la planta de enriquecimiento de uranio iraní de Natanz en 2010 ha sido uno de los momentos más señalados de todo este proceso. No se trata solamente de que se haya podido acceder desde el exterior al corazón de los sistemas de control de unas instalaciones críticas, sino que el método planteaba una novedad inquietante: Stuxnet abría el camino a toda una nueva generación de virus espía capaz de actuar de forma casi autónoma y con un potencial aterrador.

Pasaría mucho tiempo hasta que el propio Gobierno estadounidense confirmara la existencia de un arsenal informático preparado para eventuales ataques preventivos y dijera que Stuxnet formaba parte de dicha infraestructura. Posteriormente, se conocería que sería parte de una colaboración entre Estados Unidos e Israel. Tanto Stuxnet como Duqu, otro gusano, siguen un mismo patrón. El peligro de ambos es la casi independencia con la que estas armas cibernéticas operan. Una eventual "mutación" o una deriva inesperada podría hacerlas actuar a una escala no prevista o incluso volverlas contra sus creadores, como tantas obras de ciencia-ficción nos han adelantado (Andrades, 2013).

Stuxnet: la reconstrucción del caso

El caso Stuxnet arranca, de forma pública, en junio de 2010, cuando es descubierto por Sergey Ulasen en el ordenador infectado de un cliente de Irán. A partir de ahí, medios especializados, expertos informáticos y los principales fabricantes de antivirus empiezan a escudriñar sus líneas de código en busca de los secretos de lo que se calificó como "el virus más peligroso hasta entonces conocido".

Es el comienzo de un goteo de informaciones que, una a una, van revelando la naturaleza del programa y su alcance. Sin embargo, los orígenes verdaderos del caso se remontan a años atrás. Las claves esenciales, como la implicación de Estados Unidos o Israel en la creación de la ciberarma, o sus consecuencias en la planta nuclear de Natanz, no llegarán a revelarse mucho después. Una vez que todas las piezas del puzle encajan, se comprueba, además, la relación con hechos anteriores que parecían no tener conexión y puede verse la foto completa que muestra esta cronología.

Reconstruyendo los hechos, así ocurrió todo realmente:

3 de noviembre de 2005. Primera versión de Stuxnet propagada (a la que se llamaría Stuxnet 0.5 o "eslabón perdido" porque explica fallos en Natanz previos a la propagación de la versión conocida del virus). La mitad de los dispositivos infectados (que contenían el virus y lo transmitían) estaban en Irán. Esta versión estaba programada para dejar de ser activa el 4 de julio de 2009, 12 días antes de que la versión más conocida de Stuxnet fuese creada. Stuxnet 0.5 estaba preparado también para el sabotaje, pero, en lugar de variar la velocidad de las centrifugadoras, afectaba al funcionamiento de las válvulas que controlan el flujo de gas en las centrifugadoras y cascadas. Stuxnet 0.5 cerraba las válvulas de seis de cada 18 cascadas y modificaba otras en centrifugadoras individuales elegidas al azar para evitar que los operadores detectasen un patrón de problemas. [Fecha en la que esta información es conocida: febrero de 2013] (Symantec, 2013).

2006 Bush habría autorizado "oficialmente" en este año la Operación Juegos Olímpicos, la campaña de sabotaje contra las instalaciones nucleares iraníes a través de un sofisticado ciberataque. Antes de dejar la Casa Blanca en enero de 2010, instará a Obama a seguir con el plan iniciado [Fecha en la que esta información es conocida: junio de 2012] (Sanger, 2012).

2007 Una persona no identificada publica una muestra de código en la plataforma colaborativa del antivirus Virustotal, que más tarde resultó ser la primera variante de Stuxnet conocida (Stuxnet 0.5).

Principios de 2008. Siemens coopera con el Laboratorio Nacional de Idaho, que es parte del Departamento de Energía del Gobierno norteamericano y responsable de las armas nucleares, para identificar las vulnerabilidades de los sistemas de control que la empresa alemana tiene distribuidos por todo el mundo (Broad, Markoff y Sanger, 2010).

Finales de 2008-mitad de 2009. Primeros efectos de Stuxnet 0.5 en Natanz: el número de cascadas que estaban siendo alimentadas con gas y la cantidad de gas empleado comenzó a caer en algún momento entre enero y agosto de 2009, según la Agencia Internacional de Energía Atómica (Zetter, 2013b).

22 de junio de 2009. Primera oleada de propagación de Stuxnet 1.0 o Stuxnet: el virus empieza a infectar sistemas de pacientes cero. [Fecha en que este hecho es conocido: noviembre de 2010; la identidad de las empresas infectadas como medio de llegar a la central de Natanz no se conocerá hasta cuatro años después, en noviembre de 2014] .

16 de julio de 2009. Dimite el jefe del programa nuclear de Irán, Gholam Reza Aghazadeh. Según la agencia oficial iraní, había remitido una carta de renuncia tres semanas atrás al presidente Ahmadinejad.

17 de julio de 2009. WikiLeaks publica una nota informativa, firmada por Julian Assange, en la que revela que un "serio accidente nuclear" podía estar detrás de la dimisión de Aghazadeh (WikiLeaks, 2009).

Noviembre de 2009-febrero de 2010. Irán reemplaza cerca de 1.000 centrifugadoras IR-1 averiadas de su planta de Natanz (Albright, Brannan y Walrond, 2010).

Enero de 2010. Los investigadores de la Agencia Internacional de Energía Atómica acaban de completar una de sus inspecciones a la planta de enriquecimiento de Uranio de Natanz, comprobando que se había producido una renovación de centrifugadoras en los últimos meses a un ritmo inusual. Las estadísticas muestran que, en junio de 2009, las centrifugadoras de enriquecimiento IR-1 eran 4.920 y en noviembre esta cifra cae a 3.936; mientras que las IR-2/3/4 caen de 45 a 13 (Albright, Brannan y Walrond, 2010; Albright, 2009).

Enero de 2010. Poco después de su toma de posesión (4 de enero), Obama ordena acelerar el plan de ataque contra los equipos de la planta de Natanz. En las reuniones con Bush para preparar el traspaso de poderes, este le había instado a continuar con el plan iniciado durante su Administración. [Fecha en que se conoce la noticia: junio de 2012] (Sanger, 2012).

17 de junio de 2010. Sergey Ulasen, ingeniero de una pequeña empresa de seguridad informática bielorrusa, descubre un malware que explota una vulnerabilidad de Microsoft no conocida (día cero). Publica una nota sobre el virus[54] y envía un reporte a la compañía norteamericana, que, en un primer momento, no es atendido.

12 y 13 de julio de 2010. Las empresas de antivirus publican fichas sobre el malware, al que ya empiezan a denominar "Stuxnet"[55].

14 de julio de 2010. Siemens, cuyos autómatas programables son el objetivo de Stuxnet, tiene noticia de malware y dice que pone a un equipo a trabajar en ello (cit. en Zetter, 2010e). Durante meses permanecerá callada sin aportar información adicional (Langner, 2010d).

15 de julio de 2010. El blog de seguridad informática

Krebsonsecurity.com se hace eco del nuevo malware (Krebs, 2010).

16 de julio de 2010. Primer análisis de Symantec (Liam O'Murchu) sobre Stuxnet, entre otra información revela los países donde se producen más infecciones (Symantec, 2010a). También da a conocer que se aprovecha de la contraseña por defecto para acceder a la base de datos del sistema SCADA.

16 de julio de 2010. Microsoft publica una nota sobre la vulnerabilidad día cero que explota Stuxnet Microsoft (2010). Los siguientes días actualizará esta alerta con información y soluciones adicionales[56].

18 de julio de 2010. En España, el equipo de respuesta a emergencias informáticas de seguridad e industria (CERTSI), del Instituto Nacional de Ciberseguridad, se publica la alerta (INCIBE, 2010).

19 de julio de 2010. Stuxnet salta a los medios de la mano de la revista norteamericana Wired (Zetter, 2010e). Su reportera en temas seguridad informática, Kim Zetter seguirá en los próximos meses y años la evolución del caso, que terminará plasmando en un libro publicado en 2014.

20 de julio de 2010. Información adicional de Symantec (O'Murchu, 2010c) explicando cómo se instala Stuxnet en un sistema (aprovechando la vulnerabilidad de un archivo .lnk —o archivo de acceso directo— para diseminarse a través de USB) y cómo va dirigido contra sistemas SCADA.

22 de julio de 2010. O'Murchu (2010a) ofrece datos nuevos sobre los componentes de Stuxnet.

14 de septiembre de 2010. Symantec revela que Stuxnet no se aprovecha solo de una vulnerabilidad de día cero, sino de cuatro (O'Murchu, 2010b).

16 de septiembre de 2010. Ralph Langner, un ingeniero alemán especializado en programación de sistemas de control, publica en el blog de su compañía un artículo que concluye así:

“Bienvenidos a la ciberguerra” (2010e). Fue el primero que estableció que Stuxnet había sido creado para el sabotaje. Además, apuntaba como objetivo más probable el programa nuclear iraní.

21 de septiembre de 2010. Langner (2010b) deduce que Stuxnet no es solo un malware que se expande, sino que forma parte de una operación, cuyas etapas se atreve a aventurar (con bastante acierto).

21 de septiembre de 201. Nicolas Falliere (2010), de Symantec, explica el proceso por el que Stuxnet es capaz de infectar un sistema y permanecer oculto.

12 de octubre de 2010. Siemens participa en un foro en Roma sobre la seguridad de los sistemas SCADA y ofrece una de las primeras informaciones públicas de la compañía sobre el virus (Brandstetter, 2010; Langner, 2010a), consideradas por los expertos muy insuficientes.

15 de noviembre de 2010. Symantec publica un dosier sobre Stuxnet, recogiendo toda su investigación hasta el momento. Entre los datos nuevos, el descubrimiento de qué función del sistema SCADA afecta el virus: alteración de frecuencias Symantec (2010b).

23 de noviembre de 2010. Las instalaciones de la planta de Natanz de producción de combustible para enriquecimiento de Uranio, temporalmente suspendidas, según informe de la Agencia Internacional de Energía Atómica (2010).

29 de noviembre de 2010. El Gobierno de Irán reconoce que aceleradores de su planta de Natanz (sin nombrarla) se habrían visto dañados por un malware que afectaba a los procesos (Zetter, 2010c).

7 de diciembre de 2010. Siemens descubre 417 códigos de ataque en sus autómatas programables (Langner, 2010d).

22 de diciembre de 2010. Informe del Institute of Science and International Security reforzando la tesis del vínculo entre

Stuxnet y el mal funcionamiento de las centrifugadoras (Albright, Brannan y Walrond, 2010).

27 diciembre de 2010. En el Chaos Computer Club, Microsoft explica su trabajo para desenmascarar Stuxnet (Borland, 2010).

28 de mayo de 2012. Kaspersky descubre Flame, un malware usado para llevar a cabo ataques de ciberespionaje en países de Oriente Medio, con similitudes con Stuxnet. Puede propagarse a otros sistemas a través de la red de área local (LAN) y mediante memorias USB. Puede grabar audio, capturas de pantalla, pulsaciones de teclado, tráfico de red, conversaciones de Skype y puede controlar el Bluetooth para intentar obtener información de los dispositivos Bluetooth cercanos. Estos datos, junto con los documentos almacenados en el ordenador, son enviados a uno o varios servidores dispersos alrededor del mundo. Cuando termina, el programa se mantiene a la espera hasta que recibe nuevas instrucciones de esos servidores. Los países más afectados son Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí y Egipto.

24 de junio de 2012. El día que "Stuxnet murió" (Riau, 2012). La fecha programada para que las subrutinas de replicación dejasen de funcionar y el gusano dejara de infectar memorias USB.

26 de febrero de 2013. Symantec dice haber encontrado el "eslabón perdido": Stuxnet 0.5, la variante más antigua del malware nunca encontrada y que se remonta a 2005.

28 de junio de 2013. El general retirado, James "Hoss" Cartwright, investigado por posibles filtraciones a la prensa sobre el caso Stuxnet (Yoste, 2013). Finalmente, en 2015, se retirarán los cargos (Scarborough, 2015).

18 de noviembre de 2014. Kaspersky revela quiénes fueron los pacientes cero, es decir, las empresas infectadas en primer lugar por el virus como estrategia para llegar a introducirse en la planta de Natanz (Marvin the Robot, 2014).

10 de febrero de 2015. The Intercept, el medio que publica los

documentos de Snowden, saca a la luz un informe en el que NSA admite que Irán habría aprendido las técnicas de los ciberataques de los que había sido objeto (con Stuxnet y otros tres virus relacionados: Duqu, Wiper y Flame) y estaría en condiciones de usarlas contra objetivos occidentales (Greenwald, 2015).

Capítulo 5

Los ejércitos del futuro

> Nunca uses a un humano para hacer el trabajo de una máquina.
>
> Agente Smith, The Matrix

Aiden Pearce, también conocido como “The Fox”, “El Vigilante” o “El Justiciero”, es un guerrero solitario. Pearce, un hacker que lucha por vengar una injusticia, maneja el arma definitiva: un smartphone.

En una ciudad hiperconectada, controlada por un complejo sistema informático (ctOS), en la que absolutamente todo (desde los semáforos hasta las luces, desde los cajeros automáticos hasta el servicio de trenes, pasando por los ordenadores personales, tablets y móviles de los ciudadanos) está en red, su teléfono se convierte en la mejor herramienta de ataque.

Con su smartphone, Pearce interfiere las comunicaciones de los enemigos, hackea los mensajes privados de cualquiera con el que se cruce, activa todo tipo de dispositivos, navega de una cámara de vigilancia a otra, cambia el color los semáforos, activa pinchos y barreras en la carretera mientras huye o, incluso, provoca apagones para escapar entre las sombras. De momento, es ciencia-ficción, pero el escenario y la trama del videojuego francés Watch Dogs (Moreno, 2014), del que Pearce es protagonista, nos anticipan futuros escenarios de combate urbano cuya tecnología está, en buena medida, ya disponible. Sensores, robots, satélites, armas y uniformes militares inteligentes, junto con las redes hiperconectadas (Internet de las Cosas) y los avances en inteligencia artificial y Big Data, nos muestran cómo serán los ejércitos del futuro.

La guerra de los robots

Los hemos visto en las películas y en las novelas de ciencia-ficción, pero el uso de robots en la guerra no es ninguna fantasía. La primera vez que participaron en un conflicto fue en la segunda guerra mundial, con el rastreador de minas alemán Goliath y los Teletanks soviéticos. El Goliath era un pequeño vehículo sobre orugas (medía 1,5 metros de longitud y 56 centímetros de altura), conocido por estar presente en el desembarco de Normandía. Se le encomendaron diversas misiones; entre ellas, desactivar campos de minas tras la batalla de Kursk.

La URSS estrenó los Teletanks en combate en la guerra de invierno contra Finlandia. Se trataba de una serie de tanques no tripulados teledirigidos —controlados por radio desde otro tanque de control, a una distancia de entre 500 y 1.500 metros—, que habían sido producidos en la década de 1930 y principios de 1940.

En la actualidad, diferentes ejércitos han desarrollado diversos robots militares. Aunque Estados Unidos lidera estos programas, otros países como China, Francia, Alemania, Reino Unido, Israel y Rusia también tienen planes avanzados. De hecho, tal como apuntaba el Financial Times a raíz de la negociación del Pentágono con el Congreso para el incremento de su presupuesto, en la "guerra de los robots" nos encontramos en un escenario de competición análogo a la "carrera espacial" que Estados Unidos y Rusia mantuvieron durante la guerra fría (Dyer, 2016), con una tensión latente por no quedarse atrás en la progresiva automatización de los ejércitos.

El Departamento de Defensa de Estados Unidos, con un físico teórico al mando como es Asthon Carter, ha abierto a su vez una línea de colaboración con las compañías tecnológicas de Silicon Valley con el fin de intensificar la robotización militar. Entre otros proyectos, se ha impulsado un programa conjunto para la investigación en materiales que acelere mejoras en "ordenadores

flexibles" que puedan adaptarse al uniforme o al cuerpo de los soldados. También se trabaja en robots más ligeros y menos propensos a romperse o en tiras de sensores que puedan monitorear mejor la salud estructural de equipos militares grandes y costosos (Hempel, 2015).

A esto hay que sumar el trabajo que DARPA (Defense Advanced Research Projects Agency) viene llevando a cabo desde hace décadas, desarrollando aviones, coches y drones no tripulados o investigando el campo de la biónica y la inteligencia artificial[57]. Según los medios especializados, el Ejército norteamericano tendría más de 7.000 sofisticados sistemas de robótica de tierra para misiones tales como el reconocimiento y la detección y desactivación de bombas (SOFREP, 2016).

Pero no todos son ventajas: el principal inconveniente de la robótica es su incapacidad para adaptarse a condiciones imprevistas. Sin embargo, todo apunta a que los avances en inteligencia artificial pueden ayudar a cambiar esta situación en un futuro próximo.

Además, se pueden considerar desventajas: las limitaciones para ofrecer, en ocasiones, una fiabilidad 100 por cien (hay sensores de calor —infrarrojos— que fallan en condiciones de niebla, por ejemplo); su elevado coste (algo que las técnicas de impresión en 3D podrían llegar a reducir drásticamente en algunos casos); la durabilidad y resistencia de los equipos y el riesgo de un eventual hackeo (porque el dispositivo pueda llegar a ser o bien controlado por el enemigo, o bien espiado —como los papeles de Snowden relevaron que Estados Unidos y Reino habrían hecho con drones israelíes (Baeza, 2016)—.

La aplicación de la robótica para fines militares, lejos de la construcción de ejércitos de androides cinematográficos, está más cerca de la implantación de diversos dispositivos para mejorar la capacidad de observación, ataque y defensa de los ejércitos. En el campo de batalla, en un primer momento, los robots participaron en labores de reconocimiento, pero desde 2007, en la guerra de Irak, con la introducción del sistema SWORDS (Special Weapons Observation Remote reconnaissance Direct Action System), incorporan también armas (Shachtman, 2007).

Estos serían sus principales usos en la actualidad (Cervera, 2016):

Vehículos no tripulados. Israel, por ejemplo, cuenta con vehículos terrestres robotizados como REX, una "especie de jeep en miniatura con seis ruedas, capaz de transportar 200 kg de equipo durante 72 horas sin necesidad de repostar. Su mecanismo de control se basa en la voz: es capaz de reconocer u obedecer órdenes simples y, una vez programado, sigue a un soldado a una distancia fija con independencia del terreno. También es capaz de evacuar heridos si se le fija una camilla, y puede formar convoyes" (ibídem). Estados Unidos desarrolló el robot experimental BigDog/BullDog, un robot andador, cuadrúpedo y dinámicamente estable, diseñado para transportar cargas pesadas.

Robots de reconocimiento. Algunos de estos vehículos autónomos se emplean para labores de reconocimiento, como el SAHAR israelí, "diseñado como una pequeña excavadora encargada de localizar e inutilizar bombas trampa o minas". Se usa para patrullar una zona concreta y podrá incluso cooperar con drones aéreos para mantener una ruta o un área libre de explosivos. Los marines tienen a prueba "robots esféricos capaces de nadar y de andar en tierra para usarlos como infiltradores mecánicos y comprobar la actividad en playas donde planeen desembarcar". Rusia, por su parte, dispone de los Uran-6, una especie de tanques autónomos empleados para desactivar campos minados que se emplearon para limpiar de explosivos las ruinas históricas de Palmira, en Siria.

Robots centinela. Uno de los casos más conocidos sea tal vez el de las torres de robots-centinela que Corea del Sur desplegó en su frontera en 2010. Las máquinas, con tecnología Samsung, están equipadas con cámaras de imágenes térmicas, telémetros láser capaz de detectar intrusos, sensores de voz y están armadas con ametralladoras y lanzagranadas. Otro modelo son los Guardium israelíes, que "patrullan las fronteras de la Franja de Gaza: del tamaño aproximado de un jeep y dotados con sensores (sonido, infrarrojos, cámaras, radares, detectores de impacto), estos robots pueden patrullar de modo autónomo durante

varios días, vigilando y enviando sus datos a centros de retaguardia. En caso de ser atacados, disponen de blindaje ligero y de armas no letales y letales con las que responder; de ser necesario, pueden agruparse en 'enjambres' para atacar" (ibídem).

Barcos robots. En abril de 2016, Estados Unidos ha botado el que es de momento "el barco robot más grande del mundo" (Gady, 2016; DARPA, 2016). El ACTUV es el vehículo no tripulado de mayor superficie de la Marina. La embarcación (de 40 metros), conocida también como Sea Hunter, está diseñada para rastrear submarinos chinos y rusos. Está preparada para funcionar de forma autónoma de 60 a 90 días seguidos y vigilar grandes extensiones de territorio oceánico.

Sensores, cámaras y sistemas de detección. Los "sistemas de detección de disparos, sistemas radáricos que permiten visualizar personas a través de un muro, o nuevos sistemas biométricos de identificación individual incluso a distancia" son otros adelantos tecnológicos usados por los ejércitos de forma aislada o integrada en los robots.

Uniformes inteligentes. En ocasiones, estos mecanismos se añaden al propio uniforme del soldado. Uno de sus usos puede ser "facilitar sus datos biométricos en tiempo real a sus camaradas y superiores, para ser asistido en caso de resultar heridos". Además, "las versiones militares de las pulseras tipo FitBit no tardarán mucho en estar en los campos de batalla".

Biónica. Un paso más allá se encuentran las aplicaciones de la biónica que DARPA está desarrollando bajo la "Inicitaiva Brain". Algunos de estos usos son tan sorprendentes como: dispositivos microscópicos que se insertan en el cuerpo humano para "autosanarlo"; mecanismos para comunicar el sistema nervioso de manera inalámbrica con módulos externos artificiales (prótesis u otros dispositivos); o la transferencia de

datos entre el cerebro y el mundo digital[58].

Armas "inteligentes" y armas-robot. Un ejemplo pionero de arma "inteligente" (es decir, "que hace uso de la electrónica para funcionar") sería el XM25: un lanzagranadas que dispone de "un medidor de distancias láser que transmite su información a la granada antes del disparo: el usuario puede ajustar la distancia exacta a la que desea que haga explosión la granada en el aire. El proyectil 'cuenta' la distancia usando su propia rotación desde que deja el cañón". El programa One Shot ("un disparo") de DARPA tiene los mismos objetivos: desarrollar tecnología que amplíe el alcance efectivo de los francotiradores. Entre el "prodigio" (Sputnik News, 2016) y el "chasco" (Atherton, 2016) se encuentran las valoraciones del robot de la URSS, RS1A3 Mini Rex, un brazo articulado de 1,4 metros provisto de una cámara con estereovisión que se desplaza sobre orugas y termina en un arma que puede funcionar de modo automático y semiautomático. Para el reconocimiento y el ataque son también los robots estadounidenses TALON, pequeños tanques dirigidos por control remoto y armados para el combate.

El debate ético y legal

El uso de robots armados en una guerra plantea problemas éticos y legales muy serios. Amnistía Internacional viene impulsando, junto a otras ONG, la campaña internacional "Stop Killer Robots" ("detengamos los robots asesinos") y solicita la prohibición de armas y sistemas robóticos autónomos a través de un Tratado internacional:

Aunque las armas robóticas autónomas no se han utilizado todavía en conflictos armados, Amnistía Internacional prevé que el uso de armas "militares" que puedan funcionar sin un control humano eficaz incumpliría el derecho internacional de los derechos humanos y el derecho internacional humanitario, ya que, entre

otras cosas, violaría el principio de proporcionalidad y la obligación de distinguir adecuadamente entre objetivos civiles y militares.

En cuanto a los sistemas robóticos “menos letales”, se han desarrollado toda una serie de nuevas armas robóticas diseñadas para disparar proyectiles o esparcir substancias (granadas, sustancias químicas con gases lacrimógenos, balas de goma o dardos eléctricos). Estas armas pueden tener efectos letales, causar lesiones graves, y pueden ser utilizadas para violar los derechos a la libertad de expresión o de reunión pacífica” (Mendoza y Estévez, 2014).

En la misma línea, Las Naciones Unidas han pedido que “se prohíban los ‘robots asesinos’ antes de que puedan ser desarrollados” (Bowcott, 2015; Human Rights Watch, 2015).

Drones: matar a distancia

Por número de misiones y bajas ocasionadas (entre ellas, un buen número de civiles), los robots con mayor presencia en la guerra son los vehículos no tripulados de combate aéreo (UCAV, por sus siglas en inglés), más conocidos como "drones". Asimismo, son los que se llevan una mayor parte del presupuesto militar: el Pentágono tenía asignados 3.000 millones de dólares para la compra de nuevos aparatos en el año 2016 (Shaw, 2014). El pionero fue el MQ-1 Predator, un vehículo aéreo no tripulado desarrollado durante los años noventa por la Fuerza Aérea estadounidense y que se usó en la guerra de los Balcanes para tareas de reconocimiento. El Predator pasó de ser, en un principio, un sistema de vigilancia, a convertirse en un vehículo aéreo no tripulado de ataque a tierra cuando se le instalaron misiles Hellfire y sistemas de combate.

En la actualidad, los MQ-9 Reaper (anteriormente llamados Predator B) tienden a ir sustituyendo a los anteriores. Son unos aviones más grandes, pesados y más capaces: el aumento de potencia permite que el Reaper lleve 15 veces más carga útil de artillería, triplicando la velocidad del MQ-1. Ambos aviones son monitoreados y controlados por la tripulación aérea de la estación de control de tierra o GSC (ground control station).

Además de los grandes aparatos para misiones de combate, hay drones más ligeros que se usan, por ejemplo, como "plataformas de sensores". Es el caso de los estadounidenses RQ-11 Raven, el RQ-20 Puma o el diminuto Wasp III, "aviones teledirigidos lanzados a mano capaces de navegar por sí mismos y de enviar imágenes ópticas e infrarrojas a estaciones de control en primera línea" (Cervera, 2016).

El Switchblade es "un avión teledirigido diseñado para ser transportado dentro de un macuto estándar, plegado dentro de un tubo; pesa apenas 2,7 kg y desplegado mide 61 centímetros de largo. Además de un sistema de control de vuelo GPS capaz de

dirigir el aparato a unas coordenadas concretas y de una cámara en color, el Switchblade lleva una cabeza de combate equivalente a una granada de 40 milímetros, diseñada para minimizar los daños colaterales: esto significa que el aparato no se limita a mirar, sino que puede atacar al enemigo actuando como kamikaze". "El Switchblade, más que un aparato espía, sería una munición con capacidad de acecho, aunque su autonomía es muy escasa: apenas 10 minutos, ya que lleva un motor eléctrico" (ibídem). Otros países disponen de micro-UAVs comparables, por ejemplo, "los ZALA 421-08 y ZALA 421-12 rusos, el Skylite y la familia Bird-Eye israelíes y el Bayraktar turco" (ibídem).

Los avances técnicos son constantes. No hace mucho, DARPA lograba que un dron cuadrirrotor fuese capaz de salvar obstáculos a unos 72 kilómetros por hora. El proyecto "pretende que estos nuevos drones tengan un tamaño reducido para hacerlos pasar por una ventana y, a la vez, que alcancen velocidades altas sin que siquiera necesiten comunicarse con su operador ni recurran al GPS"[59].

La autonomía progresiva de estos robots aéreos parece imparable. La Marina norteamericana ya ha conseguido un avión no tripulado de combate, el X-47B, "controlado únicamente por algoritmos matemáticos" (Saiz, 2013). Está diseñado para aterrizar en la cubierta de un portaaviones, una de las maniobras más difíciles de la aviación, "no solo sin un piloto en la cabina, sino sin piloto en absoluto" (Hennigan, 2012). La ausencia de control humano en el X-47B, incluso para despegar y aterrizar, "marca un cambio de paradigma en la guerra, que es probable que tenga consecuencias de largo alcance"[60].

Cómo se hackea un dron

Uno de los retos técnicos y estratégicos que plantean los aviones no tripulados es el de su seguridad. A pesar de su uso generalizado, se sabe que sus sistemas tienen fallos.

En 2011, un virus informático tipo keylogger (que captura los golpes en un teclado para robar contraseñas) infectó las redes utilizadas por los operadores de drones en Estados Unidos. La revista Wired informó que el spyware se había resistido a los esfuerzos para eliminarlo de los ordenadores en las cabinas de mando en la Base de Creech (Nevada), donde los pilotos vuelan de forma remota drones Predator y Reaper en lugares como Irak y Afganistán. No hubo informes confirmados de que hubiera sido robada información clasificada o de que el virus impidiera misiones de vuelo. Tampoco estaban seguros de si el virus era parte de un ataque dirigido o, accidentalmente, había infectado las redes, pero fue una brecha de seguridad importante (Shachtman, 2011).

Muchos de los Reapers y Predators no cifran el vídeo que transmiten a las tropas estadounidenses de tierra. En el verano de 2009, las fuerzas estadounidenses descubrieron “días y días y horas y horas” de imágenes de sus aviones no tripulados en ordenadores portátiles de guerrilleros iraquíes. Una pieza de software de apenas 26 dólares había permitido a los yihadistas capturar el vídeo (Shachtman, 2009).

Estados Unidos y Reino Unido, por su parte, habrían espiado los drones militares de Israel. Documentos de Snowden publicados en enero de 2016 revelaron que estos países piratearon aeronaves no tripuladas desde Chipre (Baeza, 2016). Más inquietante aún que el espionaje resulta la posible pérdida de control de un dron por un hackeo. En el congreso de seguridad Rooted CON se demostró que los drones de Parrot se podían secuestrar, enviando cualquier orden al dron sin que el piloto se diera cuenta de que está siendo atacado (Sánchez, 2016).

Daños colaterales

El 17 de septiembre de 2001, seis días después del atentado contra las torres gemelas, el presidente George W. Bush firmó un nuevo MO.N (Memorandum of Notification) antiterrorista. Los MO.N son documentos altamente clasificados con órdenes específicas del

presidente a la CIA en los que se describen el ámbito y la necesidad de una operación. Entre sus disposiciones, un párrafo corto autorizaba "asesinatos selectivos" de Al Qaeda y sus aliados. El lenguaje era "simple y crudo", según su redactor, John Rizzo, entonces al frente de los servicios jurídicos de la Central de Inteligencia. Ese párrafo se convirtió en la base para las operaciones de aviones no tripulados de la CIA (Coll, 2014).

Desde entonces, se ha pasado de "un puñado de aviones no tripulados antes del 11 de septiembre de 2001" a suponer más de un tercio de todos los aviones del Ejército, "convirtiéndose en un arma central para los militares y la CIA en su lucha contra los terroristas en el Oriente Medio" (Hennigan, 2012). Las bajas estimadas por estos ataques, de acuerdo con el seguimiento que realiza la organización periodística independiente con base en Londres, The Bureau of Investigative Journalism[61], se cuentan por miles, muchas de ellas civiles. En Pakistán, por ejemplo, desde 2004 se habrían producido 423 ataques con drones, con un número de víctimas mortales de entre 2.497 y 3.999 personas, de las que serían civiles entre 423 y 965. Se calcula que los niños muertos habrían sido entre 172 y 207. Los datos recogidos por el Bureau of Investigative Journalism sobre Yemen, Somalia y Afganistán, aunque algo menores, reflejan un porcentaje igualmente significativo de muertes de civiles y niños. Los medios informan de cifras similares: en 2011, la revista Wired ya hablaba —citando a The Washington Post— de 230 ataques con drones en Pakistán, en los que habrían muerto "más de 2.000 supuestos militares y civiles"[62].

"Los modelos utilizados por la CIA —el Predator y el Reaper— parecen gigantes insectos voladores robóticos, con alerones inusuales y salientes como antenas. Los pilotos los dirigen y disparan misiles mientras están sentados delante de monitores de vídeo. Durante una misión de la CIA sobre Pakistán, un piloto podría estar en una base en Jalalabad, Afganistán, o tan lejos como en Nevada"[63], declaraba uno de ellos a la revista The New Yorker.

Situada al noroeste de Las Vegas, en el desierto de Mojave, la base aérea de Creech, en el Estado de Nevada, ha jugado un papel clave en el programa estadounidense de aviones no tripulados. Allí,

pilotos en cubículos miran a sus pantallas, donde ven la imagen de la cámara del dron y manejan un joystick para dirigirlos y disparar. En una de sus paredes cuelga una imagen de los atentados a las torres gemelas.

Brandon Bryant, un antiguo operador de aviones no tripulados, ahora se dedica a explicar su papel "en la guerra encubierta de la CIA", denunciado la despersonalización de los ataques, la deficiente información en la que se basan y las numerosas bajas civiles que provocan: "Es solo apuntar y hacer clic", cuenta Bryant[64]. Cuando dejó "honorablemente" la Fuerza Aérea, tras haber servido, entre 2005 y 2011, como piloto de drones e instructor, hizo un gesto que nunca olvidará: abrió el sobre del informe en el que se recogía el número de muertes en las que había participado durante todo ese periodo: 1.626 (Pilkington, 2015). Él, como otros expilotos, están sufriendo lo que, en términos asépticos, se denomina PTSD (post-traumatic stress syndrome) o trastorno por estrés postraumático. Una dolencia psicológica que está causando numerosas bajas en el programa de drones (Chatterjee, 2015) y que el Ejército ya está abordando (incluyendo programas de DARPA para su predicción)[65].

Antes que Bryant y sus compañeros, Heather Linebaugh, que sirvió en la Fuerza Aérea entre 2009 y 2012 como analista de imágenes y analista geoespacial para misiones en Irak y Afganistán, había denunciado en 2013 las consecuencias del programa de drones en The Guardian y otros medios. Linebaugh, entre otros detalles, explicaba la deficiente calidad de la imagen pixelada que reciben de la cámara del dron para dirigir un ataque: "Siempre nos preguntamos si matamos a la persona adecuada" (Linebaugh, 2013).

En octubre de 2015, The Intercept publicó una amplia información sobre las misiones del Ejército y los servicios de inteligencia norteamericanos con aviones no tripulados, "Drone Papers" (Reed, 2015), a partir de nuevos documentos secretos pertenecientes a la CIA y al Mando Conjunto de Operaciones Especiales (JSOC, en sus siglas en inglés). Más de 165 personas inocentes asesinadas por drones en solo un año durante una operación militar en Afganistán o el 90 por ciento de "daños colaterales" (personas inocentes muertas) en otra operación de cinco meses en Yemen son "algunas

de las escalofriantes estadísticas que se han filtrado", según valoraba El Confidencial, uno de los muchos medios que se hicieron eco de las revelaciones: "La nueva información filtrada y publicada por 'The Intercept' muestra los enormes fallos de esta estrategia y el sistema que utiliza el Ejército estadounidense para decidir, muchas veces aleatoriamente, quién vive y quién muere" (Teknautas, 2015).

Big Data, inteligencia artificial y 'machine learning'

La "guerra de los robots" dará un salto cualitativo con los progresos en inteligencia artificial que se están produciendo. Las máquinas, basándose en esta evolución, han demostrado en algunos casos superar la capacidad del hombre para "razonar" y tomar decisiones[66], mucho más allá del método de la "fuerza bruta" (hacer muchas operaciones lógicas en muy poco tiempo) en el que se basan los ordenadores tradicionales.

Ejemplos como Alpha Go, el programa desarrollado por Google (Google DeepMind) para el juego de mesa Go (cuya estrategia no depende de cálculos de probabilidades como el ajedrez —porque son infinitas—, sino de un análisis más "humano") y que llegó a vencer al mejor jugador del mundo (Peirano, 2016a) ilustran el camino hacia el que nos dirigimos.

Las Redes Neuronales Artificiales (RNA)

¿Cómo "aprende" una máquina? Hasta ahora, la capacidad de un ordenador, autómata programable o cualquier otro dispositivo electrónico de realizar cualquier tarea, por sofisticada que fuera, dependía de algoritmos programados por seres humanos.

Sin embargo, en los años cuarenta se abre un nuevo enfoque cuando el neurobiólogo McCulloch y el estadístico Pitts (1943) presentan un trabajo pionero en el que proponen un modelo matemático de tratamiento de información para una neurona artificial que "imita" a su homónima biológica:

La neurocomputación es una aportación más al viejo objetivo de crear sistemas inteligentes, considerando como tales a máquinas capaces de llevar a cabo tareas que exhiben alguna de las características asociadas a la inteligencia humana. En las dos últimas décadas, los avances en este campo han sido espectaculares; en particular el desarrollo de las redes neuronales artificiales (RNA). Originalmente, los trabajos en RNA surgen de la idea de que para que las máquinas puedan llevar a cabo dichas tareas inteligentes, sería conveniente que el modelo de computación se asemejara más a la fisiología del cerebro humano que al modelo computacional vigente […] (Alonso y Calonge, 2001).

Es decir, la idea ahora no es "programar" a una máquina para que, en base a la secuencia de órdenes introducidas realice una tarea, sino que aprenda a realizarla a partir de la información que recibe. Así, cabe distinguir dos modos o fases en el funcionamiento de una red neuronal artificial (RNA): entrenamiento (puede ser aprendizaje dirigido o no dirigido) y reconocimiento.

La fase de entrenamiento o aprendizaje se basa en el tratamiento de entradas en grandes cantidades (Big Data), es decir, "la red aprende utilizando ejemplos" (ibídem). Luego, en la fase de reconocimiento, la RNA procesa entradas correspondientes a la aplicación real, siendo capaz de reconocer patrones, clasificar (clustering) o incluso predecir resultados.

Que un dron pueda dirigirse sin ser pilotado a un objetivo mediante reconocimiento de imágenes o que una cámara de tráfico detecte comportamientos anómalos en una vía de circulación son ejemplos de tareas que las máquinas ya pueden llevar a cabo basándose en las redes neuronales artificiales.

Aclarando conceptos

En el campo de lo que globalmente se denomina "inteligencia

artificial" se manejan diferentes conceptos que conviene diferenciar (Hodjat, 2016; Alonso y Calonge, 2001):

Inteligencia artificial. Es una rama de la informática que se ocupa de algoritmos inspirados en diversas facetas de la inteligencia natural. Incluye la realización de tareas que normalmente requieren la inteligencia humana, tales como la percepción visual, el reconocimiento de voz, la resolución de problemas o la traducción de idiomas. La inteligencia artificial se puede ver en muchos productos cada día, desde el asistente personal de nuestro smartphone (Siri), a la cámara Kinect X-box 360, que permite interactuar con los juegos a través del movimiento corporal. También hay ejemplos bien conocidos de inteligencia artificial que son más experimentales, como el coche sin conductor, ampliamente discutido. Otros ejemplos incluyen la capacidad de extraer información a través del análisis de millones de imágenes.

Big Data. Es una parte importante de la inteligencia artificial y se define como conjuntos extremadamente grandes de datos cuya enorme dimensión impide que sean analizados, buscados o interpretados utilizando métodos tradicionales de tratamiento de datos. Por eso, son analizados computacionalmente para revelar patrones, tendencias y asociaciones. Sin embargo, el procesamiento de grandes volúmenes de datos para hacer predicciones o decisiones a menudo requiere el uso de técnicas de machine learning.

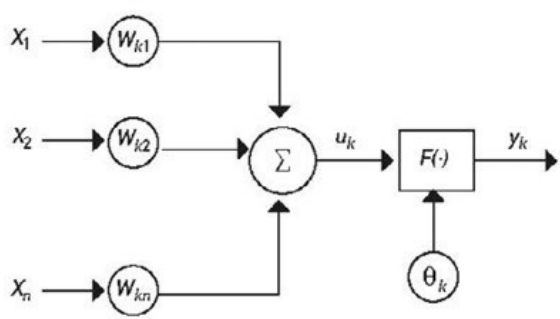
Machine learning. Es una forma de inteligencia artificial que involucra algoritmos que pueden aprender de los datos. Tales algoritmos operan mediante la construcción de un modelo basado en inputs y el uso de esa información para hacer predicciones o decisiones, en lugar de seguir las instrucciones programadas solamente de forma explícita (tal como hasta ahora hacía la computación tradicional). Las técnicas de machine learning se utilizan, por ejemplo, en la detección de spam, la identificación de fraudes con tarjetas de crédito y los sistemas de recomendación de productos, como por ejemplo con Netflix o Amazon.

Deep Learning. Es una clase de técnicas de machine learning que operan mediante la construcción de numerosas capas de abstracción para ayudar a clasificar los inputs (entradas de información) con más precisión. Las abstracciones hechas por los métodos de Deep Learning se parecen a menudo al funcionamiento del cerebro humano, y el gran avance en este campo en los últimos años ha sido el grado de abstracción que ahora se puede lograr. Esto ha dado lugar a mejoras en visión artificial y reconocimiento de lenguaje oral. El Deep Learning está inspirado en un modelo simplificado de la forma en que se cree que las redes neuronales funcionan en el cerebro.

El cine ya nos ha mostrado la capacidad de máquinas inteligentes en un escenario de ciberguerra. Los fundamentos de Skynet o del superordenador W.O.P.R., de la película Juegos de Guerra (WarGames) ya parecen estar más de cerca de las posibilidades de la tecnología que de la ciencia-ficción. Y debemos ser conscientes de ello.

FIGURA 4

NEURONA 'ARTIFICIAL'



Fuente: McCulloch-Pitts (1943), citado por Alonso y Calonge (2001).

Big Data, drones y cibervigilancia

Entre los “Drone Papers” que The Intercept filtró sobre las operaciones de Estados Unidos con aviones no tripulados, se incluye uno de apariencia anodina: un estudio titulado “Apoyo a Operaciones ISR en Somalia/Yemen”. En inglés, las siglas ISR hacen referencia a Intelligence, Surveillance and Reconnaissance, “Inteligencia, Vigilancia y Reconocimiento”. El informe fue producido por consultores de IBM para el Departamento de Defensa en 2013.

Tres años antes, en 2010, expertos en Big Data de IBM entregaron al Departamento de Defensa una presentación sobre análisis de datos dirigida a “las comunidades de defensa e inteligencia”, que The Intercept también desvela. El objetivo de IBM era explicarles cómo la compañía podría ayudarles con “la gestión de grandes volúmenes de datos” para obtener ideas “de valor incalculable”. Es decir, IBM estaba llevando al ámbito militar y de inteligencia lo que había aprendido de la gestión de grandes volúmenes de datos para las corporaciones norteamericanas” (Schwarz, 2015).

The Intercept concluye que, cuando se examina el estudio secreto ISR, se ve que el programa de aviones no tripulados del Pentágono utiliza, para elegir los objetivos de sus ataques, “el análisis de datos casi exactamente del mismo modo que IBM recomienda a las empresas que utilicen para realizar un seguimiento de sus clientes. La única diferencia significativa se produce en el final del proceso con un avión no tripulado, cuando al cliente se le mata”.

Sospechosos preventivos

El Big Data, en manos de los servicios de inteligencia, no solo sirve para poner en la diana a objetivos de ataques con drones. De una forma más indiscriminada y masiva, distintos países (entre los que se encontraría España, donde recientemente se ha inaugurado un centro con la finalidad de “coordinar, desarrollar e implantar bases de datos, sistemas de información y de comunicaciones utilizados por las Fuerzas de Seguridad del Estado”[67]) utilizan las técnicas de tratamiento de datos para establecer perfiles de supuestos

sospechosos en función de patrones determinados.

Desde el punto de vista jurídico, estas técnicas ilustran una peligrosa tendencia: la que apunta a un modelo penal "prospectivo", en el que cuenta no lo que has hecho sino lo que podrías llegar a hacer. Según este modelo, "el solo hecho de encajar en un perfil puede suponer pérdida de derechos", como apuntan los profesores de derecho penal Manuel Maroto y Adán Nieto (2013) en "Las redes sociales de Internet como instrumento de control penal", un artículo previo al caso Snowden en el que ya avanzaban los riesgos del "Estado vigilante": "Ese tipo de prácticas fulminan el principio de culpabilidad y de presunción de inocencia e institucionalizan patrones racistas y clasistas, y son un instrumento de exclusión contra el que hay que enfrentarse urgentemente" (cit. en Quintana, 2014d).

Capítulo 6

La ciberguerra de la información

La misión de un soberano, sea un monarca o una asamblea, consiste en el fin para el que fue investido con el soberano poder, que no es otro sino procurar la seguridad del pueblo.

Hobbes, Leviatán, Capítulo XXX

— ¿Durante cuánto tiempo desea que estos mensajes se mantengan en secreto? […]

— Quiero que se mantengan en secreto tanto tiempo como los hombres sean capaces de hacer el mal.

Neal Stephenson, Cryptonomicon

A lo largo de la historia, la información ha jugado un papel esencial en el desarrollo de las contiendas. Lo muestran numerosos ejemplos que van desde el espionaje y la llamada "inteligencia de señales" (SIGINT) —obtención de información mediante la intercepción de señales, bien de la comunicación entre personas, bien de señales electrónicas— hasta la difusión de mensajes destinados a confundir al enemigo, levantar la moral de los propios combatientes o condicionar negociaciones con aliados u oponentes (propaganda), al tiempo que se impide que se propaguen aquellos menos convenientes mediante la censura.

En la "era digital", los objetivos de estas actividades no han cambiado en una ciberguerra, pero sí adquieren una nueva dimensión por el potencial (y las vulnerabilidades) de las tecnologías. Una realidad que se ha puesto particularmente de manifiesto con las revelaciones del llamado "caso Snowden".

Ciberespionaje: las claves del caso Snowden

La distopía de los autores ciberpunk, un mundo donde todos somos vigilados y la tecnología se convierte en una amenaza, parece tomar vida cuando se leen, uno tras otro, los métodos y técnicas desarrollados por la NSA para construir un sistema de espionaje total.

El periodista norteamericano Glenn Greenwald estuvo a punto de perder la exclusiva de su vida por no manejar herramientas básicas de cifrado que permitieran a quien entonces era una fuente anónima, Edward Snowden, facilitarle de forma segura decenas de documentos secretos (Quintana, 2014a). Finalmente, Greenwald ha ido narrando, tanto en medios (primero en The Guardian y más tarde en su propia cabecera, The Intercept) como en el libro donde recopila los principales hallazgos, cada uno de los procedimientos empleados por la agencia norteamericana de inteligencia.

Con la descripción minuciosa de estos programas, Greenwald pretende ilustrar la filosofía "atrápalotodo" que impregna todas las actividades y programas de la NSA: "El mero hecho de tener capacidad para obtener estas comunicaciones se ha convertido en sí mismo en otro fundamento lógico para hacerlo", argumenta el escritor. Y también llamar la atención sobre el riesgo que representa: "Desde la época en que Internet empezó a usarse ampliamente, muchos han detectado su extraordinario potencial […]. La libertad en Internet […] es fundamental para el cumplimiento de esa promesa. Por tanto, convertir Internet en un sistema de vigilancia destruye su potencial básico; peor aún: transforma la red en un instrumento de represión…", advierte en las primeras páginas de Sin un lugar donde esconderse.

En última instancia, más allá de las ventajas económicas y de la manipulación diplomática, un sistema de espionaje omnipresente permite a Estados Unidos seguir controlando el mundo. Cuando Estados Unidos sea capaz de saber todo lo que están haciendo,

diciendo, pensando y planeando todos sus propios ciudadanos, poblaciones extranjeras, empresas internacionales, otros dirigentes gubernamentales, su poder sobre estos grupos y organizaciones será máximo, lo cual es doblemente cierto si el Gobierno funciona con dosis cada vez mayores de secretismo. El secretismo crea un espejo unidireccional: el Gobierno de Estados Unidos ve lo que hace todo el mundo, incluida su propia población, y nadie ve las acciones del Gobierno. Es el desequilibrio supremo, el que permite la más peligrosa de las circunstancias humanas: el ejercicio de un poder ilimitado sin transparencia ni rendición de cuentas. Las revelaciones de Edward Snowden trastocaron esta dinámica al sacar a la luz el sistema y su funcionamiento. Por primera vez, personas de todo el mundo pudieron saber el verdadero alcance de las capacidades de vigilancia acumuladas en su contra. La noticia desencadenó un intenso y prolongado debate en todo el mundo precisamente porque la vigilancia supone una grave amenaza para la gobernanza democrática. También suscitó propuestas de reforma, una discusión global sobre la importancia de la libertad y la privacidad en Internet en la era electrónica, y la consideración de una cuestión vital: ¿qué significa la vigilancia sin límites, para nosotros como individuos en nuestras vidas? (Greenwald, 2014).

Los programas de espionaje desvelados por Snowden

68

El 5 de junio de 2013, The Guardian publica el primero de una serie de documentos filtrados por el informático y excolaborador de la NSA Edward Snowden, que evidencian el espionaje masivo de la inteligencia norteamericana. Se trataba de una orden judicial clasificada como alto secreto que mostraba cómo el Gobierno de Estados Unidos había recopilado datos de las llamadas de los millones de usuarios de la operadora de telefonía Verizon. Desde entonces, se ha ido produciendo un goteo incesante de nuevas

filtraciones que, una vez reunidas, permiten comprender el alcance de esta vasta operación.

Los principales programas de ciberespionaje masivo sacados a la luz a partir de los papeles de Snowden han sido los siguientes:

PRISM. Programa de la NSA, operativo desde 2007, que permite la vigilancia masiva de ciudadanos de la Unión Europea mediante un acceso directo a los servidores centrales de empresas estadounidenses líderes en Internet, como Google, Microsoft, Facebook, Yahoo, Skype o Apple. La cantidad y modalidad de los datos aportados varía según la compañía. Desvelado el 7 de junio de 2013 simultáneamente por The Guardian y The Washington Post, fue el primer programa de ciberespionaje que conocimos gracias a las revelaciones de Snowden, después del caso Verizon.

El programa PRISM (o "Prisma", en español) permite el acceso de los servicios de espionaje a información masiva muy variada. Según se recoge en el PowerPoint filtrado con el que la propia NSA explicaba su funcionamiento, es capaz de obtener historial de búsquedas, contenido de correos electrónicos, transferencia de archivos, chats, fotografías, videoconferencias o registros de conexiones. Esta recogida masiva e indiscriminada de información se realiza bajo la supuesta cobertura legal de la Patriot Act (Ley Patriótica), aprobada por el Congreso estadounidense tras los ataques del 11 de septiembre y, sobre todo, de la Ley de Vigilancia de Extranjeros o FISA (Foreign Intelligence Surveillance Act), una norma de 1978 enmendada en numerosas ocasiones (la última vez en 2008). Esta ley establece un tribunal secreto (FISA Court), que es el que autoriza las operaciones de rastreo emprendidas por la NSA. Al margen del debate sobre la eficacia real para la seguridad de un Estado de esta recolección de datos "a granel", el impacto en los derechos de los ciudadanos es múltiple: no solo por la vulneración de la privacidad, sino por las consecuencias en otras libertades como las de expresión o asociación. El 28 de septiembre de 2013, The New York Times detallaba cómo se estarían definiendo perfiles sociales mediante el cruce de estos datos con otros que sí son

públicos, lo que abre la puerta a seguimientos selectivos en función de tendencias o afinidades. Aunque las compañías niegan conocer su participación en este programa (pese a que se llegó a publicar que habrían recibido millones de dólares como contraprestación), la NSA ha reiterado públicamente que son plenamente conscientes de ser parte de PRISM.

XKEYSCORE. Dado a conocer por O Globo y Der Spiegel el 20 de julio de 2013, se trata de un programa dedicado a la búsqueda y análisis del contenido y los metadatos de nuestras comunicaciones online. Tiene la capacidad de acceder, sin ningún tipo de autorización previa, a prácticamente cualquier actividad del usuario típico de Internet, según destacaba una de las diapositivas publicadas, orientadas a la formación de los analistas.

El propósito de XKEYSCORE, según explicaba unos días después The Guardian, es "permitir a los analistas buscar tanto en los metadatos como en el contenido de los correos electrónicos y otras actividades de Internet", como búsquedas, conversaciones en redes sociales o el historial de navegación. Y todo ello con un procedimiento tan sencillo como rellenar en el sistema un formulario.

Las búsquedas se pueden efectuar a partir del nombre, el número de teléfono, la dirección IP, palabras clave, el idioma o el tipo de navegador utilizado. Otra de las diapositivas muestra cómo la actividad de Internet está continuamente siendo recogida por XKEYSCORE y el analista tiene capacidad para consultar las bases de datos en cualquier momento.

Tempora. Programa de la agencia de inteligencia británica GCHQ para el acceso a redes informáticas y telefónicas, y a datos de localización, así como a algunos sistemas. Fue destapado por The Guardian el 21 de julio de 2013. El GCHQ tiene acceso a la red de cables que transportan llamadas telefónicas y el tráfico de Internet de todo el mundo, y ha comenzado a procesar grandes flujos de información personal sensible que está compartiendo con su socio estadounidense, la NSA. Almacenan grandes volúmenes de datos procedentes de cables de fibra óptica hasta

30 días para que pueda ser filtrada y analizada.

Esa operación, cuyo nombre en código es Tempora, ha estado funcionando durante unos 18 meses. En mayo de 2013, 300 analistas de GCHQ y 250 de la NSA habían sido asignados para procesar la inundación de datos capturada.

BULLRUN y EDGEHILL. Programas de los servicios de espionaje norteamericano (NSA) y británico (GCHQ), respectivamente, para eludir el cifrado online. Según la guía de la NSA sobre Bullrun, pueden vulnerar sistemas de encriptado y protocolos seguros ampliamente utilizados, como HTTPS.

Fueron dados a conocer por The Guardian, ProPublica y The New York Times el 5 de septiembre de 2013. Según sus informaciones, estas agencias de espionaje habrían "eludido o agrietado gran parte de la codificación que salvaguarda los sistemas bancarios y el comercio global y que protege datos sensibles como los secretos comerciales o los registros médicos. Además, se aseguran de que se muestren automáticamente los mensajes de correo electrónico, búsquedas en Internet, el contenido de los chats y de llamadas telefónicas, de estadounidenses y de otros, alrededor del mundo".

QUANTUM y FOXACID. Programas de ataques selectivos contra usuarios de TOR, según mostraban los documentos filtrados sobre su funcionamiento publicados el 4 de octubre de 2013. El modo en que operaban se basaba no tanto en atacar la propia red TOR como los sistemas de los usuarios que accedían a ella. "TOR es una herramienta de anonimato bien diseñada y robusta, y atacarla con éxito es difícil. Los ataques de la NSA que encontramos se hacen de forma individual y tienen como objetivo los usuarios de TOR, explotando vulnerabilidades en sus navegadores Firefox, y no la aplicación TOR directamente", aclaraba el experto en seguridad Bruce Schneier.

Tras identificar un usuario de TOR, "la NSA utiliza su red de servidores secretos de Internet para redirigir los usuarios a otro

conjunto de servidores secretos de Internet, con el nombre en clave FOXACID, para infectar el ordenador del usuario". Para ejecutar este ataque, la NSA recurriría a unos servidores secretos de alta velocidad denominados QUANTUM.

DISHFIRE. Programa para la recopilación y retención de 200 millones de mensajes de texto al día que sacó a la luz The Guardian el 16 de enero de 2014. La presentación filtrada sobre este programa (del año 2011) detalla cómo la NSA era capaz de extraer, cada día, de media, datos "de más de 5 millones de alertas de llamadas perdidas (de donde obtiene la red social de una persona y cuándo se pone en contacto)".

Y mucho más. "Detalles de 1,6 millones de cruces de frontera al día, a partir de las alertas de itinerancia (roaming); más de 110.000 nombres, mediante las tarjetas de visita (lo que también incluye la capacidad de extraer y guardar imágenes); y más de 800.000 transacciones financieras, tanto a través de pagos como del servicio que vincula las tarjetas de crédito de los usuarios con sus teléfonos", según destacaba The Guardian. Además de extraer los datos de geolocalización de más de 76.000 mensajes de texto al día.

MYSTIC. Un sistema, desvelado por The Washington Post, que permite grabar, analizar y recuperar la totalidad de las llamadas telefónicas de un país. A juzgar por los documentos conocidos, ya se habría llevado a la práctica en, al menos, un caso.

ICREACH. Buscador desarrollado en secreto por la NSA para rastrear entre miles de millones de metadatos obtenidos en sus actividades de espionaje indiscriminado. Se trata de uno de los sistemas de espionaje más graves por la cesión de millones de datos registrados a otras agencias como la CIA, el FBI o la DEA (que carecen del control y autorización excepcional con que supuestamente contaría la NSA) y porque habría servido para detenciones e interrogatorios a quienes se consideraban sospechosos "a la luz" del tratamiento de dichos metadatos. Estas prácticas vulnerarían la Cuarta Enmienda de la

Constitución norteamericana, que establece que solo se podrá ser objeto de investigación o detención por causas "razonables": "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil".

Cracking. Actividades de piratería y software malicioso contra instituciones, otras agencias de espionaje y operadores de telecomunicaciones.

En las filtraciones se han desvelado, junto con los programas de espionaje masivo, una amplia gama de ataques e intrusiones por parte de las agencias de inteligencia norteamericana y británica.

Así, el 31 de agosto de 2013, The Washington Post reveló, a través del análisis de los fondos reservados, que en 2011 la NSA había llevado a cabo hasta 231 "ciberoperaciones ofensivas". El 20 de septiembre se supo, por una información de Der Spiegel, que el GCHQ había hackeado Belgacom, una operadora belga de telefonía. El mismo diario alemán también destapó que el espionaje británico había usado páginas falsas de LinkedIn para introducir software malicioso en ordenadores de ingenieros y acceder así a la red de su compañía. Y el 15 de noviembre explicaba cómo el GCHQ "piratea" las redes de las empresas de telefonía móvil. La NSA también se introdujo sin problemas en las redes internas de Google y Yahoo para interceptar la información que circula entre los enormes centros de datos que estas compañías mantienen en el mundo, como informó The Washington Post el 30 de octubre. También habría usado cookies de Google para identificar objetivos que crackear, según desvelaba el mismo diario el 10 de diciembre. Además, el 23 noviembre de 2013, el medio de comunicación holandés NCR publicó que la NSA habría infectado 50.000 redes de ordenadores con software malicioso diseñado para robar información sensible.

Otra de las informaciones publicadas (esta vez por The Intercept) muestra los intentos de la NSA de cazar a administradores de redes. "De acuerdo con un documento secreto proporcionado por el 'whistleblower' [denunciante] de la NSA, Edward Snowden, la

agencia sigue la pista de la dirección de correo electrónico privado y cuentas de Facebook de administradores de sistemas antes de 'trastear' sus ordenadores para tener acceso a las redes que controlan". El objetivo sería "acceder a las llamadas y correos electrónicos que fluyen a través de sus redes". Uno de los documentos filtrados (con fecha de 2012) lleva el título "Yo cazo administradores de sistemas" y muestra cómo se pretendía elaborar una lista negra internacional de administradores de sistemas, no porque fuesen sospechosos de alguna actividad criminal sino porque, según decían, "¿qué mejor objetivo que la persona que ya tiene las 'llaves del reino'?". Y añaden: "La NSA quiere más que solo las contraseñas. El documento incluye una lista de otros datos que pueden ser cosechados desde los ordenadores que pertenecen a los administradores de sistemas, incluyendo mapas de red, listas de clientes o correspondencia comercial". Incluso parece que tenían intención de obtener "imágenes de gatos en actitudes divertidas con leyendas graciosas", según bromeaba quien fuera el autor de esos documentos.

Entre las actividades de piratería llevadas a cabo por la NSA, probablemente la más escandalosa sea la que se refiere a la manipulación de equipos informáticos fabricados en Estados Unidos para instalarles dispositivos de espionaje antes de ser exportados. Además, están documentados casos de espionaje económico, diplomático y de técnicas de propaganda (como la difusión en Internet de material o noticias engañosas) o de ingeniería social. En cuanto al espionaje económico y comercial, varios documentos ilustran la actividad de la NSA destinada a obtener información que le diese a Estados Unidos ventaja comercial. Entre ellos, las diapositivas que describen el programa BLARNEY, puesto en marcha en 1978, que cuenta entre sus "clientes" con departamentos y agencias económicas del Gobierno. Entre los países víctimas de este espionaje comercial se encontrarían, entre otros, Francia, Alemania, Italia y España.

Otro aspecto sorprendente es el papel de las empresas tecnológicas en el espionaje de la NSA. En una las diapositivas que se reproducen, se mencionan como "aliados estratégicos" de la agencia desde los grandes fabricantes de equipos o componentes, como IBM, Intel, Cisco, HP o Microsoft, a empresas de telecomunicaciones y

operadores como AT&T, Verizon, Motorola o Qwest. Los papeles de Snowden documentan, por ejemplo, la colaboración de Microsoft con el FBI para sortear el sistema de cifrado que habían implementado para Outlook o la capacidad de acceder sin autorización previa de la compañía a documentos y archivos de los usuarios en SkyDrive, un servicio de almacenamiento en la nube de Microsoft.

Con la manipulación de equipos, la "NSA recibe o intercepta rutinariamente routers, servidores y otros dispositivos informáticos de red que Estados Unidos exporta antes de ser enviados a los clientes internacionales". En el documento filtrado de la NSA se explica cómo la agencia les implanta instrumentos de vigilancia, los reempaqueta y los devuelve al circuito comercial.

La NSA también se emplea en prácticas de ingeniería social como las usadas por los ciberestafadores. El título del documento de la NSA que explica estos métodos es suficientemente ilustrativo: "El arte del engaño: instrucciones para una nueva generación de operaciones online". Entre estas técnicas se incluirían también la difusión de informaciones falsas, operaciones para dañar la reputación, señuelos o la infiltración. Además, se menciona "la legitimación de la violencia" o la "creación en la mente de los objetivos de experiencias que deban aceptar sin darse cuenta".

En cuanto a los objetivos específicos de la NSA, entre ellos se encuentran perfiles que pueden calificarse de "incómodos" para el sistema: desde Anonymous a organismos internacionales como las Naciones Unidas, activistas de defensa de los derechos humanos, la "red humana de apoyo a WikiLeaks" o personas que consideran con ideas "radicales". Por otra parte, en un caso que Greenwald reproduce en su libro como ejemplo, se recomienda explotar las "vulnerabilidades de las conductas privadas", como la visión de contenidos explícitamente sexuales online o "cargar una cantidad de dinero exorbitante por sus conferencias".

Los documentos de Snowden también han permitido conocer otros programas o herramientas destinados igualmente a la recogida masiva de datos o a su rastreo.

Boundless Informant. Destapado por The Guardian, es una herramienta que detalla en tiempo real, e incluso mapea, la información que está siendo recogida de las redes informáticas y telefónicas por la NSA.

Evil Olive y Shell Trumpet. Son programas de recogida de metadatos a gran escala.

Stellar Wind. Dado a conocer simultáneamente por The Guardian y TheWashington Post, es un programa puesto en marcha durante el Gobierno de Bush (2001) y que estuvo operativo hasta 2011. Consistía en la recogida "a granel" del registro de los correos electrónicos y del tráfico de Internet de ciudadanos norteamericanos.

Fairview. El diario brasileño O Globo informó de este programa por el que la NSA obtendría acceso a los registros de llamadas telefónicas, correos eléctricos y tráfico de Internet que se produjesen fuera de su ámbito de seguimiento. Esto se lograría, según los documentos de la propia agencia de espionaje, mediante acuerdos comerciales de una empresa de telefonía norteamericana colaboradora en el programa con las operadoras locales.

Upstream. Programa capaz de interceptar el tráfico telefónico y de Internet de los principales cables y enrutadores, tanto nacionales como extranjeros. Upstream funcionaría en paralelo con el programa PRISM.

Mainway y Association. Programas empleados por la NSA, en combinación con DISHFIRE, para interceptar las comunicaciones de la presidenta de Brasil, del presidente de México y sus respectivos ministros.

FASCIA. Titánica base de datos de la NSA con miles de millones de registros de localización a partir del seguimiento de las ubicaciones de teléfonos móviles de todo el mundo.

IMPACTO POLÍTICO DEL CASO SNOWDEN

Durante seis meses, el Parlamento Europeo, a través de la Comisión de Libertades Públicas, estuvo analizando las consecuencias para los derechos y libertades de los ciudadanos europeos del espionaje de la NSA develado por Snowden (Quintana, 2014g; 2014h).

El Parlamento Europeo da por demostrada “la existencia de sistemas tecnológicamente muy avanzados, complejos y de amplio alcance, diseñados por los servicios de inteligencia de Estados Unidos y de algunos Estados miembros, para recopilar, almacenar y analizar datos de comunicaciones, incluido el contenido, y datos y metadatos de ciudadanos en todo el mundo, a una escala sin precedentes, y de una manera indiscriminada y no basada en sospechas”.

Frente a esta realidad, la Comisión LIBE destaca que “la intimidad no es un lujo, sino la piedra angular de una sociedad libre y democrática”. Además, apuntan más lejos al sugerir “la posible existencia de otros fines ajenos a la lucha antiterrorista” como “el espionaje político y económico”.

El informe concluye que “los sistemas de vigilancia masiva indiscriminada por parte de los servicios de inteligencia constituyen una seria injerencia en los derechos fundamentales de los ciudadanos”, que estos programas pueden repercutir gravemente “en la libertad de prensa, de pensamiento y de expresión y en la libertad de reunión y asociación”, y que “implican acciones ilegales por parte de los servicios de inteligencia”. En este sentido, el Parlamento Europeo alerta “contra la instauración de un Derecho penal preventivo” y advierte que “las leyes y los tribunales secretos atentan contra el Estado de derecho”, en alusión al funcionamiento habitual de la NSA.

El Parlamento Europeo insta a los Estados miembros a que “prohíban las actividades de vigilancia masiva generalizada”, a que “cumplan de inmediato con su obligación […] de proteger a sus ciudadanos de la vigilancia […] llevada a cabo por terceros países” y a “que emprendan acciones de inmediato, incluidas acciones judiciales, contra el ataque a su soberanía […] perpetrado a través de programas de vigilancia masiva”.

En cuanto a las empresas tecnológicas como Google, Microsoft, Yahoo, Facebook, Apple y LinkedIn, el informe del Parlamento Europeo “expresa su preocupación” porque no hayan cifrado ni la información ni las comunicaciones que fluyen entre sus centros de datos, permitiendo de ese modo a los servicios de inteligencia interceptar información.

Quién es quién en el caso Snowden

Edward Snowden

Informático norteamericano de 33 años que ha desempeñado distintas funciones para los servicios de inteligencia. Su último trabajo fue como analista de infraestructura en la NSA, a través de la empresa Booz Allen. En mayo de 2013 abandonó su casa y su familia en Hawái para viajar a Hong Kong, donde facilitó al periodista Glenn Greenwald y a la documentalista Laura Poitras los documentos (entre 15.000 y 20.000) que demuestran y explican los programas de espionaje de las agencias de inteligencia estadounidense y británica. El Gobierno de Estados Unidos ha acusado a Snowden del "robo de bienes del Estado" y otros dos cargos bajo la Ley de Espionaje de 1917. Cada uno de ellos conlleva una sentencia máxima de 10 años de prisión. Su identidad fue dada a conocer el 9 de junio de 2013, después de que las primeras filtraciones ya hubieran salido a la luz, en una vídeoentrevista publicada por el diario The Guardian. Desde 2013 reside en Rusia, país que le concedió asilo político tras pasar 39 días en la zona de tránsito del aeropuerto de Moscú, a donde llegó procedente de Hong Kong. Ha recibido numerosas distinciones, entre otras, el llamado "Nobel Alternativo" (Right Livelihood Award) o el Premio Bjørnson de la Academia noruega de Literatura y Libertad de Expresión, además del reconocimiento de instituciones como el Parlamento Europeo, de organizaciones de defensa de los derechos humanos, como Amnistía Internacional y de la gratitud unánime de la comunidad de Internet, que se pone de manifiesto en cualquiera de los actos en los que participa.

Glenn Greenwald

Periodista estadounidense que destapó para The Guardian la historia del espionaje masivo de la NSA a partir de los

documentos filtrados por Snowden. Durante diez años ejerció como abogado en casos de derechos constitucionales y civiles. Columnista y analista político, primero en Salon y, después, en The Guardian, fue definido por The Atlantic como uno de los 25 comentaristas políticos más influyentes del país. Es autor de cuatro libros, tres de ellos incluidos en la lista de bestsellers de The New York Times (dos sobre el Gobierno de Bush y los abusos de su política exterior, y el tercero sobre las desigualdades en el acceso a la justicia). Ha recibido varios premios y reconocimientos, entre otros el de la Asociación de Periodismo Online 2010 por su investigación sobre el arresto y la detención de Manning. A finales de 2012, Snowden contactó anónimamente con Greenwald, con poco éxito. Sería después, a través de la documentalista Laura Poitras, como le llegarían los documentos que el informático obtuvo de la NSA. En octubre de 2013, Greenwald dejó su colaboración con The Guardian para fundar, junto con Laura Poitras y el también documentalista Jeremy Scahill, un nuevo medio financiado por Pierre Omidyar, fundador de eBay: The Intercept, lanzado el 10 de febrero de 2014. En su quinto libro, No Place to Hide: Edward Snowden, the NSA and the US Surveillance State, narra los pormenores del caso. En su comparecencia ante la Comisión de Libertades Públicas del Parlamento Europeo declaró: "La mayoría de los gobiernos de todo el mundo no solo están dando la espalda a Edward Snowden, sino también a sus responsabilidades éticas". Ha recibido distintos reconocimientos por su trabajo desvelando los papeles de Snowden, entre otros, el Premio George Polk 2013.

David Miranda

Pareja del periodista Glenn Greenwald, fue detenido e interrogado durante nueve horas en el aeropuerto londinense de Heathrow el 18 de agosto de 2013, aplicándole la legislación antiterrorista británica. Mientras estuvo retenido se le requisaron los dispositivos electrónicos que portaba: un portátil, tarjetas de memoria, su teléfono móvil y DVD. Miranda viajaba de Berlín (donde había visitado a Laura

Poitras) a Río de Janeiro, su lugar de residencia. Aunque una primera sentencia estableció que la detención estuvo justificada desde el punto de vista de la seguridad nacional, otra posterior consideró que se había producido una vulneración de la libertad de información.

Laura Poitras

Documentalista estadounidense. En sus obras denuncia los abusos y la violación de derechos de su Gobierno, particularmente en la política exterior, lo que le ha ocasionado retenciones e interrogatorios constantes. Esta circunstancia, junto con su trayectoria de denuncia de hechos no cubiertos por los medios mayoritarios, favoreció que Snowden contactara con ella en enero de 2013 para facilitarle los documentos de la NSA. Es, junto a Greenwald, Daniel Ellsberg y otros periodistas y activistas, una de las fundadoras de la Freedom of the Press Foundation, constituida en 2012, y del medio digital The Intercept. En 2014 recibió un Oscar al mejor documental por CitizenFour, en el que narra los pormenores del caso.

Sarah Harrison

Periodista británica, investigadora legal y editora de WikiLeaks. Trabaja con WikiLeaks desde que fue asignada como periodista de apoyo al portal para gestionar sus filtraciones sobre la guerra de Afganistán por el CIJ (Centre for Investigative Journalism) en el que trabajaba. Harrison acompañó a Edward Snowden en el vuelo desde Hong Kong a Moscú mientras era buscado por el Gobierno de Estados Unidos y permaneció con él en la zona de tránsito hasta que Rusia le concedió asilo.

Ewen MacAskill

Corresponsal de Defensa e Inteligencia en The Guardian. Participó, junto a Greenwald, en la publicación de las primeras filtraciones de Snowden. Por este trabajo fue nombrado coganador del Premio George Polk 2013.

James Clapper

Director nacional de inteligencia de Estados Unidos. Coordina, bajo las órdenes de Obama, las agencias de inteligencia del país. En marzo de 2013, en una comparecencia en el Senado, negó que la NSA recopilase y almacenase datos masivos de los estadounidenses. El 21 junio envió una carta de disculpa en la que aclaraba: "Mi contestación fue claramente errónea y pido disculpas por ello".

Keith B. Alexander

Director de la NSA desde 2005 y comandante del Mando Cibernético de Estados Unidos desde 2010 hasta que salieron a la luz los documentos de Snowden. Impulsor de la estrategia de recopilar información de forma masiva e indiscriminada, se le atribuye la frase: "En lugar de buscar una aguja en un pajar, recojamos el pajar completo". Presentó su renuncia a finales de 2013 para ser sustituido por el vicealmirante de la Marina, experto en criptografía y ciberguerra, Michael Rogers. Se dedica a la consultoría a empresas estratégicas sobre seguridad informática. Su tarifa: un millón de dólares.

Iain Lobban

Director desde 2008 del GCHQ hasta que se dieron a conocer las filtraciones de Snowden. Fue el impulsor del programa Tempora (crackeo de los cables de comunicación submarinos).

LA CIBERVIGILANCIA EN ESPAÑA

69

La interceptación de comunicaciones está regulada en el artículo 39 de la Ley General de Telecomunicaciones que, en su punto dos, dispone: “Los operadores están obligados a realizar las interceptaciones que se autoricen […]”. Esta autorización podrá sortearse “en caso de urgencia” para determinados delitos (delitos relacionados con la actuación de bandas armadas y elementos terroristas o rebeldes) y por un límite de 72 horas, cuando el juez deberá revocar o confirmar la orden de interceptación. La interceptación legal de las comunicaciones afecta no solo a las llamadas, sino a todas ellas, tal como contempla el artículo 39.4 de la LGT (Ley General de Telecomunicaciones): “El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles”.

Esto se realiza en España mediante la red SITEL. Un sistema del que tienen centros tres unidades del Estado (Policía Nacional, en el complejo de Canillas; la Guardia Civil y el Centro Criptológico Nacional, que pertenece al CNI) y que permite acceder a los contenidos y a los metadatos de las comunicaciones, pero solo en los casos que la ley contempla y previa autorización judicial. Sin embargo, hay abogados que consideran que “una cosa es la teoría y otra la práctica” y existe la sospecha de, por ejemplo, interceptaciones previas a la autorización del juez destinadas precisamente a obtener indicios que justifiquen la petición de “pinchazo”. El problema de SITEL, para el abogado Carlos Sánchez Almeida, es que “es un software en manos de la Policía. No lo tienen las operadoras, ni está en dependencias judiciales. Las interceptaciones se realizan desde oficinas de la Policía. Para que el agente le dé al botón solo hace falta que llegue un Auto”.

Precisamente, la falta de control fehaciente por parte de juez en parte del proceso (el volcado a DVD de las conversaciones interceptadas) motivó que, en 2010, dos magistrados del Supremo, Manuel Marchena Gómez y José Manuel Maza Martín, cuestionaran la legalidad del sistema.

¿Se intervienen demasiadas comunicaciones, o solo las necesarias? A diferencia de otros países como Alemania, Grecia, Portugal, Holanda o Reino Unido, en España el Gobierno no publica las estadísticas oficiales de las interceptaciones que se realizan, pero se puede estimar que el total de interceptaciones superan las 100.000 al año. Aunque hay quien maneja otras "cifras oficiosas" según las cuales en España existirían hasta "un millón de líneas pinchadas". Para el abogado Carlos Sánchez Almeida, "lo que estos datos demuestran es que los jueces dictan autos por encima de lo aconsejable, contraviniendo la Constitución española. La interceptación es la medida más restrictiva de la intimidad. Para que pueda aplicarse se debe dictar un auto motivado que, según la doctrina del Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos, solo puede aplicarse para delitos graves y se debe fundamentar en el peligro para la seguridad pública". "Sin embargo, en ocasiones, se aplica para delitos con una pena muy baja, como los de propiedad intelectual, y jurídicamente no está justificado. La Policía en ocasiones emplea un 'truco', que es recurrir artificialmente a la figura penal de pertenencia a grupo criminal que, según la última reforma del Código Penal, es la unión de más de dos personas que tenga por finalidad o por objeto la perpetración concertada de delitos o la comisión concertada y reiterada de faltas. Aunque finalmente los procesados queden absueltos de esa acusación, ha permitido, en el momento de solicitar al juez la interceptación, inclinar la balanza", explica Almeida. "Es como añadir un poco más de carne para que dé el peso", concluye. La realización de escuchas telefónicas injustificadas puede terminar con la nulidad de un proceso: "Un ejemplo de escuchas ilegales es el caso Anonymous, cuando se pincharon llamadas de despachos de abogados. Después de detener a una persona y ponerla en libertad, se le continuó interviniendo el teléfono, y lo que se grabaron fueron llamadas con sus abogados. Esto es gravísimo".

Estas posibilidades de vigilancia han aumentado con reformas legales recientes como la Ley de Enjuiciamiento Criminal que, entre otras cosas, legaliza los dispositivos de rastreo, la instalación de troyanos en los dispositivos de personas investigadas o la figura del agente online encubierto que puede, incluso, promover la comisión de delitos para “cazar” a supuestos sospechosos.

PROPAGANDA, CONTRAINFORMACIÓN Y CENSURA EN EL CIBERESPACIO

La propaganda como arma de guerra ha sido objeto de decenas de estudios en el ámbito de la sociología, la política o la historia del periodismo. Con la llegada de la comunicación de masas, esa función, que históricamente se había desarrollado a través de canales directos (como los juglares) o minoritarios (los libros o los primeros periódicos), se va a multiplicar. Con la prensa de masas, y después con la radio y la televisión, los ejércitos van a contar con un arma enormemente poderosa.

Una realidad patente desde sus momentos más tempranos: "La primera guerra mundial (1914-1918) fue un laboratorio dantesco en el que se gestaron formas de entender la violencia, la comunicación y la política que acabarían marcando todo el siglo XX, y cuyas consecuencias son palpables aún en nuestros días. El empleo de armamento químico en los campos de batalla es, tal vez, la más infame de esas primeras veces. El otro gran 'hallazgo' fue el uso masivo y sistemático de la propaganda, la censura e incluso la mentira descarada al servicio de los intereses bélicos" (Máiquez, 2014). Ahora, en la nueva frontera digital, cambian los canales y las técnicas, con todo lo que ello representa, pero algunas de las estrategias y de los objetivos siguen siendo los mismos.

Hay veces que la influencia se produce en sentido inverso. En Ciberactivismo: las nuevas revoluciones de las multitudes conectadas (Tascón y Quintana, 2012) ya se menciona el impacto de las noticias sobre Internet, ofreciendo una imagen permanente de entorno peligroso, en medidas orientadas a limitar la libertad o criminalizar actividades permitidas en el mundo offline. En el caso de la ciberguerra, Stephanie Ricker Schulte (2013), en su libro Cached: Decoding the Internet in Global Popular Culture (véase también Kaplan, 2016), analiza al detalle los efectos de la cobertura mediática sobre los riesgos de un "ciberenfrentamiento" global y la

peligrosidad de la red. Un enfoque ("enmarcado", por usar el término técnico) que se acentuó a raíz del estreno de la película Juegos de Guerra (WarGames) y que habría tenido consecuencias directas en la estrategia de ciberseguridad impulsada por la Administración Reagan.

PROPAGANDA: REDES SOCIALES AL SERVICIO DE LA CAUSA

Cuando el 1 de mayo de 2011 el Gobierno norteamericano tuvo que anunciar que había dado muerte al líder terrorista Osama Bin Laden puso en marcha la habitual batería mediática: comparecencia televisiva del presidente, comunicado oficial y rueda de prensa. El principal soporte de aquella estrategia de comunicación fue la mítica foto de Pete Souza mostrando el momento en el que, desde la "Sit-Room" (sala de crisis) de la Casa Blanca, Obama, junto a miembros de su gabinete y distintos mandos militares, presenciaban en directo el ataque a través de las cámaras de aviones no tripulados que sobrevolaban el complejo de Bin Laden. Cinco años después de aquello, el 1 de mayo de 2016, la CIA publicó el siguiente mensaje en su cuenta de Twitter: "Con motivo del 5º aniversario de la operación Osama Bin Laden en Abbottabad vamos a twittear la incursión como si estuviera sucediendo hoy en día. #UBLRaid". La CIA, que cuando ocurrieron los hechos no tenía aún perfil en esta plataforma de microblogging, aprovechó la efeméride para dramatizar aquel acontecimiento e imponer su narrativa de los hechos. Es decir, una acción de "propaganda de guerra" en toda regla. La anécdota sirve para ilustrar cómo las redes sociales (igual que antes fue la fotografía, la radio o el cine) son canales con cada vez más peso en las tácticas de "información" en guerras y conflictos. Un ejemplo paradigmático de ello es el despliegue comunicativo del terrorismo yihadista.

Cómo está ganando el yihadismo la batalla de las redes sociales

Mientras que en el campo de los ataques informáticos el yihadismo, según los servicios de inteligencia, no parece una amenaza inminente (principalmente por falta de solvencia técnica para ello), no ocurre así en el terreno de la propaganda, donde ha entendido a la perfección el contexto comunicativo para explotarlo. Algunas de las claves que explican su capacidad de propaganda a través de Internet son (Koerner, 2016):

Adopción temprana: desde el inicio de sus acciones, utilizaron YouTube para difundir vídeos de sus atentados por atroces que fueran.

Manejan múltiples soportes: desde una revista en inglés de cuidado diseño que distribuyen como pdf a través de redes sociales (Dabiq), a perfiles en las principales plataformas de social media.

Difusión transmedia: multiplican el impacto social de cualquier acción, "explotándola" en todas los canales en los que están presentes: redes sociales como Twitter o Facebook, aplicaciones de mensajería como Telegram y Surespot y plataformas para compartir contenidos como JustPaste.it.

Acciones descentralizadas: actualizan sus canales con contenidos realizados de forma autónoma por adeptos de múltiples procedencias geográficas.

Uso intensivo de las redes de comunicación y actualizaciones de contenido frecuentes en diferentes formatos: 38 nuevos artículos por día, vídeos de 20 minutos, largometrajes documentales, ensayos fotográficos, clips de audio y folletos.

Multilingüe: los contenidos que difunden en Internet se publican en idiomas que van del ruso al bengalí.

Utilizan estrategias de viralización idénticas a las que usan las marcas o medios populares como Buzzfeed, como crear contenido variado para llegar a "audiencias nicho".

Uno de estos “nichos” de audiencia son los enclaves musulmanes específicos en todo el mundo. A ellos les dirigen mensajes triunfalistas al estilo de la propaganda tradicional. Más allá de los vídeos atroces por los que son conocidos, el mayor porcentaje de los contenidos que difunden se destina a mostrar la grandeza de lo que llaman “Estado Islámico” mediante imágenes de proyectos de obras públicas, desarrollo económico y triunfos militares. Los resultados que recogen los informes que analizan el yihadismo dan cuenta de su eficacia: la propaganda digital de este tipo “ha ayudado a motivar a más de 30.000 personas a dar la espalda a todo lo que siempre han conocido y viajar miles de millas a tierras peligrosas, donde les han dicho que un paraíso les espera”.

Los mensajes no solo sirven para ganar partidarios, sino para disuadir a oponentes: “Los vídeos de escuadrones de la muerte del ISIS, persiguiendo y asesinando a personal de seguridad iraquí, ayudaron a persuadir a la policía y los soldados de otras ciudades a desaparecer en lugar de resistir”.

Transparencia y publicidad mejor que secreto, diferenciándose así de otros grupos extremistas islámicos previos como Al Qaeda.

La producción distribuida (crowdsourcing) de contenido se completa con una gestión “profesional” de los nodos principales a los que se va accediendo por una especie de meritocracia.

Servicios profesionales retribuidos (como cámaras) y medios técnicos avanzados para la realización de material audiovisual que en ocasiones busca la narrativa y estética de los videojuegos.

Se busca conectar con la audiencia potencial: en lugar de comunicaciones que ponen el acento en los líderes, como Al Qaeda, el protagonismo lo tienen los combatientes de base: “Ese cambio de perspectiva narrativa ha puesto al Estado Islámico en sincronía con una generación que está acostumbrada a crear y compartir su propio contenido. Cuando los espectadores jóvenes echan un vistazo a los vídeos del Estado Islámico, a continuación, pueden imaginarse a sí mismos allí mismo en la pantalla”.

Censura. En las zonas bajo su control cortan el acceso a cualquier tipo de información que no sea producida por la propia red. Los

expertos lo resumen así: “Hoy, el Estado Islámico es más un conglomerado mediático que una fuerza de lucha” (ibídem).

CONTRAINFORMACION: EL CASO DE WIKILEAKS

En el contexto de un conflicto, las acciones de contrainformación serían, en un sentido amplio, aquellas estrategias comunicativas que se ponen en marcha para contrarrestar el discurso del oponente e imponer una narrativa propia. Aunque cualquier agente de la ciberguerra puede iniciar este tipo de campañas, quienes cuentan con canales de comunicación poderosos y tienen capacidad de imponer un discurso dominante (gobiernos, empresas…) tienen menos necesidad de moverse en este terreno e intervienen en la guerra de la información desde la propaganda. Por eso, la encontraremos la contrainformación en los márgenes del poder.

Sin duda, el fenómeno más relevante que se ha producido en este campo es el de WikiLeaks, el portal de filtraciones fundado en 2006 por Julian Assange. En 2008 empieza a publicar “las primeras filtraciones importantes, e incluso recibe su primera orden judicial de cierre, que le hace famoso ante la mayoría de los hacktivistas de todo el mundo”. El impacto “a gran escala” de WikiLeaks llegaría en 2010 por la publicación masiva (más de 250.000 documentos) de comunicaciones diplomáticas secretas (los “cables diplomáticos”) que revelaban escándalos políticos de todo tipo y que afectaban a numerosos países. El 28 de noviembre se difundieron 291 de los 251.287 documentos obtenidos por WikiLeaks desde el servidor de la organización y, de manera simultánea, en cinco grandes medios de referencia que habían tenido acceso previo a los mismos: El País (España), Le Monde (Francia), Der Spiegel (Alemania), The Guardian (Reino Unido) y The New York Times (Estados Unidos).

WikiLeaks demostró ser un eficaz revulsivo como herramienta de contrainformación: “El Cablegate, como toda buena crisis, pone muchas cosas patas arriba”, dice Margarita Padilla (2012) en su libro El kit de la lucha en Internet, en el que analiza con detalle el alcance del fenómeno. Por un lado, WikiLeaks abrió un debate

sobre la transparencia y la libertad de prensa. En segundo lugar, a través de una "alianza monstruosa" con medios de comunicación no marginales, sino de referencia, visibilizó su verdadera condición: "La crisis del Cablegate ha tocado y hundido al periodismo de investigación convencional que, de repente, en una semana, ha envejecido siglos"; también pone de manifiesto "la connivencia de la prensa 'mainstream' con la corrupción generalizada"; además, aunque se sirve de los medios, está demostrando al mismo tiempo que ya no son necesarios; y, por último, les obligó a tomar partido en la campaña de acoso que Estados Unidos emprende contra el portal, con el resultado previsible (mostrarles como un elemento más de un sistema que parte de la sociedad ve ya como decadente). En tercer lugar, WikiLeaks demostró cómo debe ser la "contrainformación" en una sociedad en red:

La contrainformación hoy es publicar aquello que van a querer ocultar y poder analizarlo para que la ciudadanía lo entienda. Los colectivos no necesitan de un Indymedia para decir lo que hacen. Para eso ya están los blogs. Como estrategia para ganar visibilidad, el modelo portal está en claro retroceso. La gente no se va a leer los cables enteros, de igual forma que no se va a leer la Ley de Economía Sostenible entera. No es problema. Si no puedes ser WikiLeaks, tienes que ser un intermediario que sea capaz de destacar información y llevarla a la ciudadanía. Esa es la contrainformación del siglo XXI: o revelas secretos o los analizas (Txarlie, Hacktivistas) (citado en Padilla, 2012).

CENSURA

Las posibilidades de Internet para acceder y difundir información, para organizarse y crear redes, y como arma para ataques, según hemos ido viendo a lo largo del libro, hace que los gobiernos, incluso los democráticos, de forma temporal o constante, impongan limitaciones para acceder a algún tipo de contenido o servicio online (o a la propia red). Turquía, con el cierre de servicios como

Twitter, YouTube o la red TOR; Venezuela, con Pastebin o Zello; y Reino Unido, con el bloqueo del sistema de mensajería de Blackberry durante los disturbios de 2011, son algunos ejemplos de censuras "puntuales". En otros países, en los que no existe libertad de información de ningún tipo, la censura a Internet es permanente.

Para lograrlo, se emplean diversas técnicas, como el filtrado, el bloqueo de webs, la alteración de la velocidad de la navegación, e incluso ataques informáticos como los de denegación de servicio (DDoS) y el robo de contraseñas. Las restricciones pueden ser impuestas por distintos agentes (desde una institución pública, como una universidad o una biblioteca, a empresas y gobiernos) y aplicarse a cualquier punto de la red. Así, pueden afectar a la "columna vertebral" de Internet (lo que condiciona el acceso a la red en todo un país), a los ISP o proveedores de acceso a Internet (normalmente, las órdenes de filtrado de los gobiernos son ejecutadas por estos), a redes institucionales o al equipo personal del usuario (como con los programas de control parental).

Cómo se censura en Internet: distintos tipos de bloqueo y filtrado[70]

Las técnicas de filtrado suponen, por lo general, el uso de software para ver lo que los usuarios están tratando de hacer y de interferir selectivamente en sus actividades, es decir, que "la censura y la vigilancia están en la práctica íntimamente ligadas", como advierte uno de los manuales más completos sobre el tema. Por eso, las contramedidas técnicas más eficaces se van a basar en el uso del cifrado o en el empleo de servicios seguros que dificultan el rastreo.

Los distintos tipos de bloqueo y cifrado se han usado (y se usan) en distintos momentos por un gran número de países. Por eso, aunque a continuación se mencionan algunos ejemplos que ilustran dichos métodos, conviene consultar los "perfiles de país" de la iniciativa OpenNet para una visión detallada de cada caso o el informe "Enemigos de Internet", de Reporteros Sin Fronteras. También se puede recurrir a Herdict, una plataforma colaborativa que recoge en tiempo real situaciones de censura en Internet.

Filtrado de URL. Una forma que tienen los países y otras entidades para

bloquear el acceso a la información en la web es evitar el paso a una dirección URL completa (o a parte de ella). En ocasiones, las autoridades son más selectivas y el bloqueo solo afecta a ciertos subdominios de un dominio particular. Por ejemplo, la lista de sitios web prohibidos en China contempla el bloqueo de secciones específicas, dejando el resto del dominio accesible. O el caso de Vietnam, donde el Gobierno bloquea las versiones en vietnamita de la BBC y de Radio Free Asia, pero no los contenidos escritos en inglés.

Filtrado o suplantación de DNS (Domain Name System). Cuando se introduce una URL en un navegador web, lo que hace el explorador es preguntar al servidor DNS por la dirección numérica que corresponde a esa URL y así poder suministrar la correspondiente dirección IP. Si el servidor DNS está configurado para bloquear el acceso, consulta una lista negra de nombres de dominio prohibidos. Cuando un navegador solicita la dirección IP de uno de estos nombres de dominio, el servidor DNS da una respuesta de error o ninguna respuesta. El resultado, en todo caso, es que los servicios bajo un nombre de dominio particular, o todas las páginas en un servidor web en particular, no estarán disponibles. Otro método es la redirección de los usuarios a sitios web incorrectos. Esta técnica se denomina "DNS spoofing", y puede usarse para suplantar la identidad de un determinado servidor y mostrar los sitios web falsos o desviar el tráfico de los usuarios a otros servidores que podrían interceptar sus datos. Ha sido empleada en Turquía para evitar que los usuarios accedieran a Twitter y YouTube a través de servidores DNS públicos de Google, como estaban haciendo para evitar el bloqueo de esos servicios. También se usó en Túnez para el robo de contraseñas o el phishing de Gmail y también en Siria, para suplantar páginas de Facebook de activistas.

El filtrado de IP. Para evitar que los usuarios accedan a servidores específicos, pueden configurar los routers para que no transmitan los datos destinados a las direcciones IP en una lista negra o para que devuelvan un mensaje de error. De este modo, se bloquean todos los servicios proporcionados por un servidor en particular, tanto las páginas web como el correo electrónico. Fue el sistema que, según la EFF, se habría aplicado en Venezuela para impedir el acceso a imágenes en

Twitter o a Pastebin, una aplicación web que permite subir pequeños textos y que estaba siendo usada por Anonymous (como en otras ocasiones) para difundir formas de evitar la censura.

Filtrado de palabras clave. Se usa de forma adicional a otras formas de bloqueo. Se inspecciona el intercambio de información (paquetes) por palabras clave, interrumpiendo la transmisión cuando se detecta una de las calificadas como prohibidas.

Análisis de paquetes (DPI) para modulación del tráfico. Otro método de censura es reducir la velocidad de acceso a determinados contenidos o servicios. Usado, por ejemplo, por Rusia, se basa en dar prioridad a algunos tipos de paquetes y en retrasar otros. Esta técnica es utilizada a veces por las compañías que dan acceso a Internet (ISP) en contra de las redes para compartir archivos.

Bloqueo de puertos. Los servicios en Internet (acceso web, correo electrónico, mensajería instantánea, etc.) tienen números de puerto característicos. Si un puerto está bloqueado, todo el tráfico en este puerto se convierte en inaccesible. Por ejemplo, un censor puede bloquear solo el puerto 80, que es el utilizado normalmente para el acceso web. A menudo se bloquean los puertos 1080, 3128 y 8080, porque estos son los puertos más usados por los proxy (servidores intermediarios empleados para eludir los bloqueos).

Apagado de Internet. La forma de censura más absoluta es el cierre de la conexión a Internet. Los primeros países en cerrar el acceso a Internet por completo fueron Nepal, en 2005, y Birmania, en 2007. Egipto cortó por completo el acceso a Internet entre el 27 de enero y el 2 de febrero de 2011. El cese de la actividad fue absoluto, aunque algunos usuarios encontraron formas de sortearlo. Otros países que emplearon la misma táctica fueron Libia, con cortes intermitentes, Bahrein (que incrementó su filtrado, pero no cerró totalmente el acceso a la red) y Siria.

Censura de los proveedores de servicios. A veces, las autoridades pueden inducir a los operadores de servicios a cooperar con la censura. Google, por ejemplo, publica semestralmente las solicitudes que recibe para borrar contenido de sus servicios.

Ataques DDoS. Los ataques de denegación de servicio bloquean un sitio de Internet mediante una sobrecarga por exceso de solicitudes de comunicación en un momento preciso. Fueron empleados por Bielorrusia en las elecciones de 2010 contra el sitio de información opositor Charter97.

También son, igualmente, formas de censura: la anulación de nombres de dominio, la desconexión de servidores, las restricciones para el acceso privado a Internet o la vigilancia de nuestro tráfico para aplicar después medidas penales. Más grave es la persecución o encarcelamiento de bloggers, como en Vietnam, Rusia o algunos países árabes, cuyo número supera ya al de periodistas de medios, según el Barómetro de la Libertad de Expresión de Reporteros Sin Fronteras. Es el caso, por ejemplo, del egipcio Alaa Abd El-Fattah —condenado en 2015 a cinco años de prisión— o del saudí Raif Badawi —Premio Sajarov a la libertad de expresión y condenado en 2012 a diez años de cárcel, al pago de un millón de riales saudíes y a mil latigazos por "difamar al islam"—. Por último, no podemos olvidar los efectos de censura (o "autocensura") que tienen los sistemas de espionaje o rastreo digital: se da así una contradicción entre las nuevas posibilidades que ofrecen los canales digitales para saltarse los filtros tradicionales y poder difundir con mayor libertad, y una realidad menos utópica por las facilidades que estas propias herramientas ofrecen para perseguir cualquier tipo de disidencia[71].

LAS GUERRAS DEL CIFRADO

72

El cifrado (encryption, en inglés, de ahí su frecuente traducción errónea como “encriptado”) ha saltado en los últimos tiempos al debate público. Sin embargo, los métodos de cifrado se han utilizado durante siglos por diplomáticos, oficiales de inteligencia y soldados para enviar mensajes confidenciales sin temor a que los contenidos pudieran leerse si eran interceptados.

El término “criptografía” se refiere a la práctica y al estudio de la teoría y técnicas para el almacenamiento y comunicaciones seguras. El cifrado es el proceso real de la combinación de los contenidos de un mensaje (“texto plano”) con un valor secreto o clave (la “llave” de cifrado), de tal manera que sustituye el contenido por otro totalmente nuevo (“texto cifrado”) que es ininteligible para los usuarios no autorizados. El objetivo es que solo alguien con la llave correcta pueda descifrar la información y convertirla de nuevo en texto plano. El cifrado moderno se basa en algoritmos matemáticos para proteger la seguridad y la integridad de los mensajes y de flujos de datos, cuando son transmitidos electrónicamente o cuando se almacenan en dispositivos.

En la historia contemporánea de la guerra, el cifrado ha dado momentos míticos. Es el caso del código secreto Enigma, usado por el Ejército alemán en la segunda guerra mundial y que “Alan Turing fue el principal responsable de descifrar, contribuyendo con ello a acortar la guerra. Turing inventó una máquina, llamada la ‘bomba’, que permitía descifrar mensajes Enigma de forma masiva. En 1943 se desvelaban 84.000 mensajes alemanes al mes. Sus métodos de criptoanálisis fueron decisivos para paliar la amenaza de los submarinos en la Batalla del Atlántico” (García Bejarano, 2014).

Durante gran parte del siglo XX, estas técnicas sofisticadas de cifrado estaban disponibles casi exclusivamente para los miembros

del Gobierno, militares y las comunidades de inteligencia. El envío de mensajes electrónicos cifrados se mantuvo fuera del alcance de los ciudadanos comunes hasta 1976. Todo cambió con la invención de la criptografía de clave pública en 1976. Dos investigadores, Whitfield Diffie y Martin Hellman, publicaron un trabajo revolucionario sobre una nueva tecnología, "La criptografía de clave pública", que demostraba cómo los individuos y las empresas ordinarias podrían comunicar datos con seguridad en las modernas "redes de comunicación". Su visión crucial fue que la clave utilizada para cifrar un mensaje podría estar relacionada con —pero ser distinta de— la clave utilizada para descifrar el mensaje. Por lo que cualquiera podría crear y distribuir una clave única "pública", útil solo para crear mensajes que nadie más que el propietario de la correspondiente clave "privada" sería capaz de descifrar. A diferencia de los anteriores métodos de cifrado, este enfoque permitía a dos o más partes comunicarse de forma privada y de forma segura, incluso si no se han conocido previamente.

Sin embargo, a pesar del avance que supuso el trabajo de Diffie y Hellman, durante un tiempo el cifrado permaneció aún en el estrecho círculo del debate académico. Va a ser con la extensión masiva de la informática, a través de los ordenadores personales y de las redes de comunicación, cuando el cifrado se convierta en una necesidad para un público más amplio: "El mercado de los sistemas de cifrado fuertes que finalmente se desarrolló tuvo dos factores fundamentales: el creciente uso de ordenadores personales por las grandes empresas y la demanda de tecnología de correo electrónico seguro para uso individual. Como ambas cosas se hicieron más comunes, en la década de 1980, la demanda comercial de productos de cifrado se disparó" (Kelh, Wilson y Banskton, 2015).

Mientras que en esos años las empresas estaban llevando gran parte del desarrollo comercial de la tecnología de cifrado (software de autenticación y firma digital, antivirus, protección de almacenamiento de datos, productos de seguridad de red, etc.), una floreciente comunidad de defensores de la privacidad también comenzó a crear herramientas de cifrado para los usuarios individuales. El científico de la computación Philip Zimmermann diseñó una de las primeras grandes herramientas prácticas para el cifrado de clave pública de extremo a extremo de archivos y correo

electrónico —un proyecto al que llamó “Pretty Good Privacy” (PGP) — y que lanzó públicamente en el año 1991.

Desde ámbitos militares se empezó a ver la posible adopción generalizada del cifrado como una amenaza a su monopolio. Además, complicaba el espionaje porque, con el correo electrónico, los mensajes se habían convertido en “cartas sin sobre”: postales con todas las facilidades para acceder a su contenido. Estaban decididos a impedir que eso ocurriera.

La primera guerra del cifrado

El conjunto de iniciativas puestas en marcha por el Gobierno norteamericano en los años noventa para impedir la extensión del cifrado y la correspondiente contestación por parte de usuarios, hacktivistas y organizaciones de defensa de los derechos civiles en Internet se conoce como “las guerras del cifrado”, aunque, a la luz de los acontecimientos actuales, tal vez haya que bautizarlas como “la primera guerra del cifrado”. Se libró, principalmente, en torno a dos batallas:

LA BATALLA CONTRA CHIP CLIPPER

El acto que realmente puso en marcha las guerras del cifrado fue la introducción en 1993 del Chip Clipper, un microchip desarrollado por los ingenieros del Gobierno para ser usado como un dispositivo de cifrado por las compañías de telecomunicaciones dedicadas a la transmisión de voz. El corazón de todo el concepto en torno al Chip Clipper y su algoritmo, Skipjack (desarrollado por la NSA y, por lo tanto, clasificado), era el de la clave bajo custodia. En cualquier fábrica donde se produjese un dispositivo telefónico o cualquier aparato que fuese a usar el Chip Clipper se le asignaría una “llave criptográfica” que luego sería entregada al Gobierno en “garantía”.

Si alguna agencia de Gobierno estimaba que era “necesario” escuchar algún tipo de comunicación, la llave sería “desbloqueada” y entregada a la agencia de Gobierno correspondiente para así poder descifrar las comunicaciones.

Las organizaciones de defensa de los derechos civiles como ACLU y EFF emprendieron una batalla legal contra la iniciativa por entender que el único efecto que tendría sería dejar expuestos a los ciudadanos comunes y corrientes a la posibilidad de ser vigilados ilegalmente por su Gobierno.

En 1994 —se descubrió además un fallo en el sistema de cifrado—, era una propuesta descartada y nunca llegaría a implantarse. No obstante, el Gobierno no desistió en su idea de encontrar una forma de acceder a las claves de las comunicaciones cifradas privadas.

LA BATALLA DE LAS EXPORTACIONES: EL CIFRADO COMO ARMA

El Gobierno abrió otro frente contra la extensión del cifrado al plantear si las tecnologías americanas de cifrado fuerte debían estar disponibles en el extranjero. Así iniciaron una batalla legal contra su exportación, dando a estas herramientas el mismo tratamiento jurídico que al comercio de armas. Fue una de las primeras victorias de los criptopunk (activistas que abogan por el uso generalizado de la criptografía) al sistema, al lograr, al final de aquella batalla, que se permitiera el uso de la criptografía en las comunicaciones electrónicas fuera del ámbito gubernamental. Una de las mejores crónicas de ese periodo es el relato del Steven Levy, quien narra los episodios principales en su libro Crypto: cómo los informáticos libertarios vencieron al Gobierno y salvaguardaron la intimidad en la era digital.

La difusión de PGP fuera de Estados Unidos se logró finalmente de una forma un tanto épica, que logró sortear las leyes que impedían exportaciones relacionadas con la criptografía. Zimmermann publicó todo el código fuente de PGP en un libro de tapa dura a través de MIT Press, que se distribuyó y vendió ampliamente.

Cualquier persona que quiso desarrollar su propia copia de PGP podía comprar el libro, cortar las tapas, separar las páginas y, con ayuda de determinados programas, crear un conjunto de archivos de texto de código fuente. PGP estuvo así disponible en cualquier lugar del mundo y al poco tiempo se convirtió en el sistema de cifrado más usado. Zimmermann tuvo que enfrentarse a tres años de investigación penal por esta causa.

En España, "ciberactivistas pioneros", como David Casacuberta, Carlos Almeida o Mercè Molist, integrados en comunidades como FrEE (Fronteras Electrónicas España) o Kriptópolis, hicieron una importante labor para defender y explicar la necesidad de las herramientas de cifrado para la privacidad y libertad de expresión de los internautas. En 1996 comenzó a publicarse PGP Magazine, el primer boletín electrónico sobre criptología, en internet y en castellano. Es obra de José Manuel Goméz, un aficionado no académico, autor también de La Página de PGP en Español. Un año después, pondrá en marcha otro boletín: Kriptópolis, que a finales de 1999 contaba con 14.000 suscriptores[73].

La segunda guerra del cifrado

Episodios como el de la batalla del FBI contra Apple para que esta le aportara las claves de acceso al móvil de uno de los terroristas del tiroteo de San Bernardino demuestran que estamos en una guerra del cifrado, aunque su origen se remonta bastante más atrás. Los episodios principales de esta nueva contienda son los siguientes (Geller, 2016):

9 de enero de 2003. El Departamento de Justicia norteamericano elabora la Ley de Mejora de la Seguridad Interior de 2003, también conocida como Patriot Act II. Dos años después de los ataques terroristas del 11 de septiembre de 2011 y de que se aprobara la Patriot Act, el Departamento de Justicia del presidente George W. Bush prepara un proyecto de ley, la Ley de Mejora de la Seguridad Interior de 2003, que apuntaba al cifrado de una manera importante, lo que generó la reacción de los activistas por las libertades en Internet. La Patriot Act II

nunca se convirtió en ley, pero fue la primera incursión del Gobierno en la regulación del cifrado de la época reciente, y también en un ambiente social de gran sensibilidad por la amenaza terrorista.

Agosto de 2007. Los investigadores de seguridad descubren una puerta trasera en el protocolo de cifrado apoyado por la NSA. En marzo de 2007, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) publicó un documento que describe un protocolo de cifrado en el que más tarde expertos van a detectar la existencia de puntos débiles. Finalmente, se supo que el sistema fue creado de modo que hubiera una manera de predecir el proceso de generación supuestamente aleatorio. Cualquiera que pudiera hacer esto podría descifrar los datos cifrados. En septiembre de 2013, The New York Times informó que la NSA había "empujado agresivamente" al NIST y la Organización Internacional de Normalización para adoptar este sistema como un estándar de cifrado. En diciembre de 2013, se supo que la NSA había pagado a la empresa de seguridad líder RSA diez millones de dólares para añadir este sistema a uno de sus productos, lo que habría animado a muchos otros en la industria a adoptar el código. En abril de 2014, el NIST retiró formalmente su recomendación de este sistema.

Enero de 2008. El FBI comienza a "informar" a los legisladores sobre la amenaza de cifrado. Desde principios de 2008, el FBI comienza una campaña dirigida a los legisladores para asociar cifrado con criminalidad y a transmitir a los miembros del Congreso que "la capacidad del FBI para recoger información y llevar a cabo investigaciones a través del uso de la tecnología se está reduciendo cada vez más".

4 de mayo de 2012. El FBI promueve una legislación para garantizar una intervención telefónica web-friendly ("fácilmente accesible online"). El FBI prepara un proyecto de ley para obligar a los proveedores de correo electrónico, los operadores de servicios de VoIP, clientes de mensajería instantánea y las redes sociales a modificar sus servicios para facilitar escuchas telefónicas. Al final, no se introdujo la legislación.

6 de junio de 2013. El segundo documento Snowden expone un programa masivo de vigilancia en Internet. Durante años, la NSA y el FBI han estado accediendo directamente a los servidores de las empresas

de tecnología de datos sin una orden judicial.

5 de septiembre de 2013. Documentos de Snowden desvelan la campaña de la NSA para romper el cifrado.

Septiembre de 2014. Apple y Google se suman al cifrado de disco completo de sus sistemas operativos móviles.

10 octubre de 2015. La Administración de Obama declara que no buscará una legislación de puerta trasera para cifrado.

27 de octubre de 2015. Una petición dirigida a Obama para que rechace las puertas traseras supera las 100.000 firmas.

4 de noviembre de 2015. El Gobierno británico introduce la Ley de Poderes de Investigación (Investigatory Powers Bill). Se trata de una ley con una premeditada redacción ambigua que no excluye las puertas traseras para acceder a contenidos cifrados.

13 de noviembre de 2015. Los terroristas matan a 130 personas en París. Casi inmediatamente, funcionarios estadounidenses empezaron a proponer nuevos poderes de vigilancia, incluyendo puertas traseras para los sistemas de cifrado para ayudar a la captura de los extremistas en Estados Unidos. Exjefes de inteligencia de la agencia y el líder del Comité de Seguridad Nacional de la Cámara argumentaron que el cifrado irrompible aumenta la probabilidad de un ataque exitoso. Incluso llegaron a difundir informaciones falsas, como la historia sobre una aplicación de mensajería cifrada del Estado Islámico llamada "Alrawi", que alimentaba la narrativa sobre los riesgos del cifrado irrompible.

17 de noviembre de 2015. El Congreso comienza a revisar el cifrado. La primera promesa de un presidente de la comisión para examinar la regulación del cifrado se produjo cuatro días después de los ataques de París. Algunos legisladores se refieren a la capacidad de las empresas de ofrecer cifrado irrompible como "inaceptable".

2 de diciembre de 2015. En un centro de reposo de San Bernardino (California), dos yihadistas disparan y matan a 14 personas, lo que fue el ataque terrorista más mortífero en suelo de Estados Unidos desde el 11 de septiembre del 2001. Siete días más tarde, en una audiencia del

Comité de Inteligencia del Senado con los jefes de las principales agencias de inteligencia, el jefe del FBI manifiesta que habían sido incapaces de acceder a un iPhone utilizado por uno de los tiradores, Syed Rizwan Farook (ahora fallecido).

9 de diciembre de 2015. Los líderes del Comité de Inteligencia del Senado anuncian planes para regular las "puertas traseras". La presidenta del Comité de Inteligencia del Senado anunció que están trabajando en un proyecto de ley para garantizar la capacidad de los investigadores para leer mensajes cifrados.

17 de diciembre de 2015. El fabricante del cortafuegos NetScreen revela probabilidades de puertas traseras en su código.

23 de diciembre de 2015. China declara que adapta su nueva política de cifrado a la ley de Estados Unidos: La ley antiterrorista aprobada en China contiene un lenguaje vago que podría transformarse en una obligación de dejar "puertas traseras". El portavoz del Ministerio de Asuntos Exteriores, Hong Lei, declara a Reuters que el Gobierno había modelado su legislación para adaptarse a la ley estadounidense.

27 de diciembre de 2015. Los legisladores norteamericanos de ambos partidos promueven una comisión que analice el cifrado.

4 de enero de 2016. Holanda se convierte en el primer país en rechazar formalmente las puertas traseras: "El Gobierno cree que en este momento no es deseable para tomar medidas legales contra el desarrollo, la disponibilidad y el uso de cifrado dentro de los Países Bajos". Con estas palabras, la Administración del primer ministro holandés, Mark Rutte, se convirtió en el primer Gobierno nacional en oponerse a las puertas traseras en los sistemas de cifrado.

12 de enero de 2016. Legisladores franceses consideran autorizar las "puertas traseras". Este esfuerzo fracasó dos días más tarde, cuando el secretario de Estado francés describió las puertas traseras como una "vulnerabilidad al diseño", "inapropiadas" y que no suponían "la solución correcta".

21 de enero de 2016. Legisladores de dos Estados de Estados Unidos proponen la prohibición del cifrado irrompible. California y Nueva York se convirtieron en los primeros dos Estados en instar a los legisladores

nacionales a regular las puertas traseras. La propuesta de Nueva York citó el terrorismo como la amenaza que exige la legislación, mientras que el proyecto de ley de California menciona la trata de personas.

28 de enero de 2016. El presidente del Comité de Seguridad Nacional del Senado de Ron Johnson rompió con la ortodoxia del partido cuando criticó las puertas traseras usando los mismos argumentos que las organizaciones de libertades civiles y los criptógrafos. Johnson señaló que una ley estadounidense así empujaría a los criminales a plataformas fabricadas en el extranjero, y sugirió que, después de los ataques terroristas, los estadounidenses deberían tener cuidado de no legislar "en caliente". También sugirió que el apoyo a las puertas traseras provenía de "no entender la complejidad" de la cuestión.

1 de febrero de 2016. Un juez de Massachusetts ordena en secreto a Apple ayudar a la Policía a acceder a iPhone.

11 de febrero de 2016. Un estudio pone en duda la capacidad de prohibir el cifrado irrompible. Los críticos de las puertas traseras en los sistemas de cifrado afirman que cualquier ley nacional o regional solo serviría para empujar a los criminales y terroristas hacia productos y servicios creados en otros lugares. Expertos como Bruce Schneier publican un documento titulado "Una encuesta mundial de productos de cifrado", que identifica 546 productos cifrados producidos fuera de Estados Unidos, para argumentar que un Gobierno no puede controlar el entorno del cifrado global por sí solo.

16 de febrero de 2016. La batalla legal del iPhone de San Bernardino entra en erupción: una juez de primera instancia en Riverside (California) ordena a Apple que cree una versión personalizada de su sistema operativo móvil iOS para desactivar varias características de seguridad en un iPhone 5 con iOS 9. Esa era la configuración del teléfono del tirador de San Bernardino, Syed Rizwan, al que los agentes del FBI supuestamente no podían acceder.

El CEO de Apple, Tim Cook, prometió en una carta a los clientes que su compañía lucharía contra la orden, y los abogados de Apple presentaron un escrito recurriendo la orden de la juez Pym. El Departamento de Justicia, por su parte, también se personó en la causa, apoyando la decisión de la juez. Conseguir la firmeza de la resolución era importante porque, según el FBI, "potencialmente"

podría sentar un precedente.

29 de febrero de 2016. Una juez de Nueva York niega la solicitud del Gobierno de la orden de desbloqueo de iPhone. A medida que la lucha de San Bernardino entró en su segunda semana, el juez de primera instancia en el caso de drogas de Nueva York, James Orenstein, denegó la petición del Departamento de Justicia. "El Congreso ha estudiado una legislación que permita lograr el mismo resultado, pero no lo ha adoptado", escribió Orenstein para explicar su razonamiento.

1 de marzo de 2016. Apple apela la orden judicial de San Bernardino.

1 de marzo de 2016. La polémica del teléfono del asaltante de San Bernardino llega al Congreso, donde comparecen los máximos responsables del FBI y Apple. El director del FBI, James Comey, declara que solo Apple tiene los medios para acceder al contenido del móvil. Unos días después, Snowden lo desmentirá desde su cuenta de Twitter: "Es mentira", dice el exanalista de la NSA.

3 de marzo de 2016. Google, Facebook y Microsoft se unen en la batalla legal de Apple contra el FBI. Los gigantes tecnológicos pedirán al juez que apoye al fabricante del iPhone en su negativa a piratear el móvil de un terrorista.

21 de marzo de 2016. El FBI pide un aplazamiento de la causa porque podría conseguir, "gracias a un tercero", acceder al contenido del móvil del terrorista.

28 de marzo de 2016. El FBI renuncia al caso al anunciar que ha conseguido hackear el iPhone con ayuda de una tercera parte que no especifica. El FBI se ha retirado antes de dar pie a un precedente legal que perjudicaría su batalla contra el cifrado.

La guerra continúa.

Bibliografía

Ackerman, S. (2010): “It Begins: Military’s Cyberwar Command Is Fully Operational”, Wired, 4 de noviembre [www.wired.com/2010/11/it-begins-militarys-cyberwar-command-is-fully-operational].

AIEA (2010): Informe [www.iaea.org/sites/default/files/gov2010-62.pdf http://www.wsj.com/articles/SB10001424052748704369304575633083063905598].

Albright, D.; Brannan, P. y Walrond, C. (2010): “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment”, Institute of Science and International Security (ISIS), 22 de diciembre [http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant].

Albright, D. (2009): “IAEA Report on Iran”, 16 de noviembre de 2009 [www.isisnucleariran.org/assets/pdf/ISIS_Analysis_IAEA_Report_16 Nov2009.pdf].

Alkhouri, L.; Kassirer, A. y Nixon, A. (2016): “Hacking for Isis: The Emergent Cyber Threat Landscape”, Flashpoint [www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf].

Alonso, A. (2014): “Anonymous amenaza a Lizard Squad”, eldiario.es, 29 de diciembre [eldiario.es http://www.eldiario.es/juegoreviews/noticias/Anonymous-amenaza-Lizard-Squad_0_340166450.html].

— (2015): “Dos presuntos miembros de Lizard Squad detenidos por la policía”, eldiario.es, 2 de enero [eldiario.es http://www.eldiario.es/juegoreviews/noticias/presuntos-miembros - Lizard-Squad-detenidos_0_3415 65947.html].

Alonso, L. y Calonge, T. (2001): “Redes neuronales y reconocimiento de patrones”, en L. Alonso, Reconocimiento de patrones con redes neuronales, Salamanca, Imprenta Cardenal.

Andrades, F. (2013): “Cinco escenarios de ciberguerra en el nuevo orden mundial”, eldiario.es, 7 de mayo [www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html].

Appelbaum, J. (2013): “Shopping for Spy Gear: Catalog Advertises NSA Toolbox”, Spiegel, 29 de diciembre [www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html].

Arquilla, J. y Ronfeldt, D. (1993): “Cyberwar is Coming!”, Santa Monica, Rand Corporation, Santa Monica, CA [www.rand.org/pubs/reprints/RP223.html].

— (1996): “The Advent Of Netwar”, Rand Corporation, Santa Monica, CA [www.rand.org/pubs/monograph_reports/MR789.html].

Atherton, K. D. (2016): “Russia’s War Robots Are Less Than They Appear”, Popular Science, 20 de enero [www.popsci.com/russias-war-robots-are-less-than-they-appear].

Baeza (2016): “EE UU y Reino Unido espiaron los drones militares de Israel”, El País, 29 de enero [http://internacional.elpais.com/internacional/2016/01/29/actualidad/ 1454097551_970138.html].

Ballesteros, R. (2016): “Un virus ‘ransomware’ inutiliza nueve áreas del Ministerio del Interior una semana”, El Confidencial, 3 de mayo [http://www.elconfidencial.com/espana/ 2016-05-03/un-virus-ransom ware-inutiliza-nueve-areas-del-ministerio-del-interior-una-semana_1192 757].

Barnes, J. E. (2008): “Pentagon computer networks attacked”, Los Angeles Times, 28 de noviembre [http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28].

Berger, J. (2016): “A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case”, The New York Times, 25 de marzo.

Berreby, D. (2014): “Lewis Fry Richardson‘s weather forecasts changed the world. But could his predictions of war do the same?”, The Independent, 19 de agosto de 2014.

Bohorquez, J. C.; Gourley, S.; Dixon, A. R.; Spagat, M. y Johnson, N. F. (2009): “Common ecology quantifies human insurgency”, Nature, vol. 462, 19 de diciembre [www.nature.com/nature/journal/v462/n7275/full/nature08631.html].

Borland, J. (2010): “A Four-Day Dive Into Stuxnet’s Heart”, Wired, 27 de diciembre [www.wired.com/2010/ 12/a-four-day-dive-into-stuxnets-heart].

Bort, J. (2016): “Something called ‘Google dorking’ helps hackers find out stuff no one wants them to know”, Business Insider, 1 de abril [www.businessinsider.com/google-dorking-helps-hackers-2016-4].

Bowcott, O. (2015): “Legal affairs correspondent UN urged to ban ‘killer robots” before they can be developed”, The Guardian, 9 de abril [www.theguardian.com/science/2015/apr/09/un-urged-to-ban-killer-robots-before-they-can-be-developed].

Brandstetter, T. (2010): “Stuxnet Malware Official communication presented at SANS SCADA Summit 12-10-2010” [https://files.sans.org/summit/euscada10/PDFs/08%20BrandsetterStuxnet-Communication-tb.pdf].

Brenner, S. (2013): “Cyber-threats and the Limits of Bureaucratic Control”, Minnesota Journal of Law, Science & Technology, 14 [http://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1082&context=mjlst].

Broad, W. J.; Markoff, J. y Sanger, D. E. (2010): “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”, The New York Times, 15 de enero de 2011.

Cabrerizo Calatrava, A. (2002) “El conflicto asimétrico”, Congreso Nacional de Estudios de Seguridad”, Universidad de Granada, 21-25 de octubre [www.ugr.es/~ceas/Sociedad%20y%20seguridad/CABRERIZO.pdf].

Camhi, J. (2016): “US critical infrastructure facing more cyber attacks than ever”, Business Insider, 1 de abril.

Caro Bejarano, M. J. (2013): “La nueva dimensión de la amenaza global: la amenaza cibernética”, Boletín del Instituto de Estudios Estratégicos (IEES), julio [www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA40-2013_AmenazaCibernetica_MJC.pdf].

Cartledge, J. (2015): “Isis terrorist Junaid Hussain killed in drone attack after boffins ‘crack group’s code’”, Birmingham Mail, 16 de septiembre [www.birminghammail.co.uk/news/midlands-news/isis-terrorist-junaid-hussain-killed-10069425].

CCDCOE/OTAN (2016): “Cyber Security Strategy Documents”, 6 de abril [https://ccdcoe.org/cyber-security-strategy-documents.html].

Centro Criptológico Nacional (2016): “Informe anual: Ciberamenazas 2015. Tendencias 2016” [www.ccn-cert.cni.es/informes/informes-de-amenazas-ia/ 1475-ccn-cert-ia-09-16-ciberamenazas-2015-tendencias-2016/file.html].

Cervera, J. (2016): “Miras, sensores, drones y robots: la infantería del futuro ya está aquí”, El Confidencial, 7 de marzo [www.elconfidencial.com/tecnologia/2016-03-07/las-armas-y-tecnologias-que-usaran-los-soldados-del-futuro_1163875].

Chatterjee, P. (2015): “A chilling new post-traumatic stress disorder: Why drone pilots are quitting in record numbers”, Salon, 6 de marzo [www.salon.com/2015/03/06/a_chilling_new_post_traumatic_stress_disorder_why_drone_pilots_are_quitting_

Coll, S. (2014): “The Unblinking Stare”, The New Yorker, 24 de noviembre [www.newyorker.com/magazine/2014/11/24/unblinking-stare].

Crawford, D. y Solomon, J. (2010): “Iran Nuclear Sites Temporarily Suspended”, The Washington Post, 24 de noviembre [www.wsj.com/articles/SB10001424052748704369304575633083063905598].

Cox, J. (2016): “US Charges Iranians With Coordinated Cyber

Attacks on Banks, Companies", Motherborad, 24 de marzo [http://motherboard.vice.com/read/us-charges-iranians-with-coordinated-cyber-attacks-on-banks-companies].

Cuthbertson, A. (2016): "Isis Hackers Target The Wrong Google" Newsweek, 1 de marzo [http://europe.newsweek.com/isis-hackers-target-wrong-google-431911?rm=eu].

D'Amico, M. L. (1999): "Hackers spar over cyber war on Iraq, China". CNN, 13 de enero [http://edition.cnn.com/TECH/computing/9901/13/cyberwar.idg].

Dang, B. (2010): "27C3: Adventures in analyzing Stuxnet", intervención en el CCC, 28 de diciembre [www.youtube.com/watch?v=rOwMW6agpTI].

DARPA (2016): "Deputy Secretary of Defense, Senior U.S. Navy Leadership Join DARPA Director to Christen ACTUV Prototype Vessel", DARPA News, 11 de abril [www.darpa.mil/news-events/2016-04-11].

Departamento de Defensa de Estados Unidos (2009): "Base Structure Report. Fiscal Year 2009 Baseline" [www.defense.gov/Portals/1/Documents/pubs/BSR2009Baseline.pdf].

Dougherty, C. y Hamilton, J. (2014): "Ex-NSA Chief Pitches Banks Costly Advice on Cyber-Attacks", Bloomberg, 20 de junio [www.bloomberg.com/news/articles/2014-06-20/ex-nsa-chief-pitches-advice-on-cyber-threats-to-the-banks].

Dyer, G. (2016): "US military: Robot wars", Financial Times, 7 de febrero [www.ft.com/intl/cms/s/2/849 666f6-cbf2-11e5-a8ef-ea66e967dd 44.html#axzz46d nVNtQ].

Electronic Frontier Fundation (s. f.): "The Crypto Wars: Governments Working to Undermine Encryption" [www.eff.org/document/crypto-wars-governments-working-undermine-encryption].

Elola, J. (2011): "Somos Anonymous", El País, 16 de enero.

Erdbrink, T. (2012): "Facing Cyberattack, Iranian Officials

Disconnect Some Oil Terminals From Internet", The New York Times, 23 de abril [www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0].

Escorcia, A. (2013): "Demostración del ataque a #YaMeCanse y #USTired2", Loquesigue TV [www.youtube.com/watch?v=_V1LcFCB7zs].

Estado Mayor Conjunto de los Estados Unidos (2013): "Cyberspace Operations", Joint Publication 3-12 (R), febrero de 2013 [www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf].

Falliere, N. (2010): "Exploring Stuxnet's PLC Infection Process", Symantec, 21 de septiembre [www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process].

Finley, K. (2015) "Pro-Government Twitter Bots Try to Hush Mexican Activists", Wired, 23 de agosto [www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists].

Fisher, M. (2013): "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?", The Washington Post, 23 de abril.

Fojón, E. (2016): "A vueltas con la atribución cibernética", Ciber Elcano, nº 11, Real Instituto Elcano y THIBER, febrero [www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-11-febrero-2016].

Gady, F. (2016): "World's Largest Anti-Submarine Robot Ship Ready for Sea-Trials in April", The Diplomat, 11 de febrero [http://thediplomat.com/ 2016/ 02/worlds-largest-anti-submarine-robot-ship-ready-for-sea-trials-in-april].

Gaffey, C. (2015): "German missiles hacked by foreign source", Newsweek, 8 de julio [http://europe.newsweek.com/german-missiles-hacked-by-foreign-source-329980].

García Bejarano, P. (2014): “Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial”, eldiario.es, 6 de febrero [http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_2260 78042.html].

Geller, E. (2016): “A complete guide to the new ‘Crypto Wars’“, The Daily Dot, 16 de abril [http://www.dailydot.com/politics/encryption-crypto-war.s- backdoors-timeline-security-privacy].

Gibson, W. (2007): Neuromante, Ediciones Minotauro, Madrid.

Gómez Delgado, A. (Fanta) (2013): “Border Check: herramientas de la lucha por la neutralidad de la red”, El Diagonal, 28 de octubre [www.diagonalperiodico.net/saberes/20495-border-check-herramientas-la-lucha-por-la-neutralidad-la-red.html].

Goncharov, M. (2012): “Russian Underground 101”, Trend Micro Incorporated [www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf].

Gonsalves, A. (2012): “Bank attackers more sophisticated than typical hacktivists, expert says”, CSO, 28 de septiembre [www.csoonline.com/article/2132319/malware-cybercrime/bank-attackers-more-sophisticated-than-typical-hacktivists--expert-says.html].

González, M. (2013): “Nosotros no nos fiamos de nadie”, entrevista a Carlos Gómez López de Medina, jefe del Mando Conjunto de Ciberdefensa, El País, 21 de julio [http://politica.elpais.com/politica/2013/07/19/actualidad/1374244373_693749.html].

Gonzalo, M. y Quintana, Y. (2014): “Greenwald: La NSA planea usar información privada para destruir la reputación de ciertas personas”, eldiario.es, 30 de marzo [http://www.eldiario.es/turing/vigilancia_y_privacidad/Greenwald-NSA-informacion-reputacion-personas_0_265624239.html].

Gorman, S. (2012): “China Tech Giant Under Fire”, The Washington Post, 8 de octubre [www.wsj.com/article_email/SB10000872396390443615804578041931689859530-

lMyQjAxMTAyMDAwNzAwODc3Wj.html].

Gostev, A. (2014): “Agent.btz: a Source of Inspiration?”, Securelist, 12 de marzo [https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration].

Gourley, S. (2009): “Sean Gourley habla sobre las matemáticas de la guerra”, Vídeo TED, 9 de febrero [www.ted.com/talks/sean_gourley_on_the_mathematics_of_war?language=es#t -210985].

Greenwald, G. (2014): Sin un lugar donde esconderse, Ediciones B, Barcelona.

— (2015): “NSA claims iran learned from western cyberattacks”, The Intercept, 10 de febrero [https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks- learning-attacks].

Guerrero-Saade, J. A.; Raiu, C. y GReAT (2016): “Operation Blockbuster revealed”, SecureList/Kaspersky, 24 de febrero [https://securelist.com/blog/incidents/73914/operation-blockbuster-revealed].

HackStory (s. f.): “Declaración contra la ciberguerra”, [http://hackstory.net/Declaraci%C3%B3n_contra_la_CiberGuerra].

Haley, D. (2014): “Los cuatro eventos más destacados de seguridad en Internet del 2014”, Symantec, 13 de noviembre. [www.symantec.com/connect/blogs/los-cuatro-eventos-mas-destacados-de-seguridad-en-internet-del-2014].

Hempel, J. (2015): “DOD Head Ashton Carter Enlists Silicon Valley to Transform the Military”, Wired, 18 de noviembre.

Hennigan, W. J. (2012): “New drone has no pilot anywhere, so who’s accountable?”, Los Angeles Times, 26 de enero [http://articles.latimes.com/2012/jan/26/business/la-fi-auto-drone -20120126].

Hodjat, B. (2016): “Myth Busting Artificial Intelligence”, Wired/Insights, febrero [www.wired.com/insights/ 2015/02/myth-busting-artificial-intelligence/#comment-1864590868].

Human Rights Watch (2015): “Mind the Gap. The Lack of Accountability for Killer Robots”, 9 de abril [www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots].

Igarape Institute-The SecDev Foundation (2012): “A fine balance: Mapping cyber (in)security in Latin America” [https://igarape.org.br/pdf/Strategic%20Paper%202%20(June%202012).pdf].

INCIBE (2010): “Vulnerabilidad en el intérprete de comandos de Windows”, 18 de julio [www.incibe.es/securityAdvice/CERT/Alerta_Temprana/Avisos_seguridad_tecnicos/vulnerabilidad_interprete_comandos_windows_20100718].

— (2015a): “Misiles Patriot alemanes atacados”, 8 de julio de 2015 [www.incibe.es/technologyForecastingSearch/CERT/Bitacora_de_ciberseguridad/Misiles_Patriot_alemanes_atacados].

— (2015b): “Primer corte de suministro eléctrico de la historia debido a un ciberataque”, 23 de diciembre [www.incibe.es/technologyForecastingSearch/CERT/Bitacora_de_ciberseguridad/Primer_corte_suministro_historia_debido_ciberataque].

Ingersoll, G. (2013): “Inside The Clever Hack That Fooled The AP And Caused The DOW To Drop 150 Points”, Bussiness Insider, 22 de noviembre [www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused-the-dow-to-drop-150-points-2013-11].

Kaplan, F. 2016): “‘WarGames’ and Cybersecurity’s Debt to a Hollywood Hack”, The New York Times, 19 de febrero [http://www.nytimes.com /2016/02/21/movies/wargames-and -cybersecuritys-debt-to-a-hollywood-hack.html?_r = 0].

Kaspersky Lab (2014): “Stuxnet: Zero victims. The identity of the companies targeted by the first known cyber- weapon”, 11 de noviembre [https://securelist.com/analysis/publications/67483/stuxnet-zero-victims].

Kaspersky, E. (2011): “The Man Who Found Stuxnet: Sergey Ulasen in the Spotlight”, 11 de noviembre [https://

eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight].

Kelh, D.; Wilson A. y Banskton, K. (2015): “Doomed to repeat history? Lessons from the CryptoWars os 1990s”, Open Technology Insittute [https://www.newamerica.org/oti/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s].

Kershner, I. (2013): “Pro Palestinian hackers attack israelí sites”, The New York Times, 7 de abril [www.nytimes.com/2013/04/08/world/middleeast/pro-palestinian-hackers-attack-israeli-sites.html].

Khandelwal, E. (2016): “Israeli Power Grid Authority Suffers Massive Cyber Attack”, The Hackers News, 27 de enero [http://thehackernews.com/2016/01/power-grid-cyberattack.html].

Knowlton, B. (2010): “Military Computer Attack Confirmed”, The New York Times, 25 de agosto [www.nytimes.com/2010/08/26/technology/26cyber.html?_r=1&ref=technology].

Koerner, B. (2016): “Why ISIS Is Winning the Social Media War”, Wired, 16 abril.

Krebs, B. (2010): “Experts Warn of New Windows Shortcut Flaw”, Krebsonsecurity.com, 15 de julio.

Lake, E. (2012): “Who Is Behind Cyberattacks on Israel’s Airline and Banks?”, The Daily Beast, 18 de enero [www.thedailybeast.com/articles/2012/01/17/who-is-behind-cyber-attacks-on-israel-s-airline-and-banks.html].

Langner, R. (2010a): “On Siemens’ “official” Stuxnet communication: Back to the lab, please” [www.langner.com/en/2010/11/11/on-siemens-official-stuxnet-communication-back-to-the-lab-please].

— (2010b) “Ralph’s analysis, part 2”, 21 de septiembre [www.langner.com/en/2010/09/21/stuxnet-logbook-sep-21-2010-1200-hours-mesz].

— (2010c): “Ralph on cyberwar: War 0.1”, 12 octubre [www.langner.com/en/2010/10/12/stuxnet-logbook-

oct-12-2010-1100-hours-mesz].

— (2010d): “Siemens discovers 417 attack code”, 7 de diciembre [www.langner.com/en/2010/12/07/siemens-discovers-417-attack-code].

— (2010e): “Stuxnet logbook, Sep 16 2010, 1200 hours MESZ” [www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz].

— (2013): “To Kill a Centrifuge A Technical Analysis of What Stuxnet’s Creators Tried to Achieve”, noviembre [www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf].

Linebaugh, H. (2013): “I worked on the US drone program. The public should know what really goes on Heather”, The Guardian, 29 de diciembre [www.theguardian.com/commentisfree/2013/ dec/29/drones-us-military].

Lynn III, W. (2010): “Defending a New Domain. The Pentagon’s Cyberstrategy”, Foreing Affairs, septiembre-octubre [www.foreignaffairs.com/articles/united-states/2010-09-01/ defending-new-domain]. y http://archive.defense.gov/home/ features/2010/ 0410_cybersec/lynn-article1.aspx

Máiquez, M. (2014): “Propaganda sin rubor: la prensa durante la I Guerra Mundial”, 20 minutos, 1 de abril [http:// www.20minutos.es/noticia/2101331/0/primera-guerra- mundial/ prensa/propaganda/#xtor=AD-15&xts=467263].

Malenkovich, S. (2013): “Morris Worm Turns 25”, KasperskyLab Daily, 4 de noviembre [https://blog.kaspersky.com/morris-worm-turns-25/3065].

Maroto, M. y Nieto, A. (2013): “Las redes sociales en Internet como instrumento de control penal. Tendencias y límites”, en R. Martínez Martínez y A. Rallo Lombarte (dirs.), Derecho y redes sociales, Civitas, Madrid, pp. 427-484.

Martínez, V. (2015): “63 ‘ciberataques’ en lo que va de año contra

infraestructuras críticas del Estado", El Mundo, 26 de octubre [www.elmundo.es/economia/2015/10/26/562cf6c0e2704e21798b45bb.html].

Marvin The Robot (2014): "El origen de Stuxnet", Kaspersky Lab, 18 de noviembre [https://blog.kaspersky.es/el-origen-de-stuxnet/4887/C].

— (2015): "La epidemia del ransomware: por qué deberías estar preocupado", Kaspersky Lab, 15 de julio [https://blog.kaspersky.es/ask-expert-ransomware-epidemic/6439].

Matthews, G. (2016): "Google Search Technique Aided N.Y. Dam Hacker in Iran", The Wall Street Journal, 27 de marzo [www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543].

McCarthy, N. (2015): "Birmingham hacker Junaid Hussain killed in Syria drone strike, US military claims", Birmingham Mail, 26 de agosto [www.birminghammail.co.uk/news/birmingham-hacker-junaid-hussain-killed-9935890].

Meer, H. (2013): "Cyberwar, Stuxnet and people in glass houses", Al Jazeera, 7 de junio [www.informationclearinghouse.info/article28275.htm].

Mendoza, I. y Estévez, A. (2014): "Robocop y Terminator, cada día más cerca", eldiario.es, 28 de noviembre.

Menn, J. (2013): "Cyber attacks against banks more severe than most realice", Reuters, 12 de mayo [www.reuters.com/article/us-cyber-summit-banks-idUSBRE94G0ZP201 30518].

Microsoft (2010): "Microsoft Security Advisory 2286198: Vulnerability in Windows Shell Could Allow Remote Code Execution", Microsoft TechNet, 16 de julio [https://technet.microsoft.com/library/security/2286198].

Mills, E. (2012): "What do Stuxnet, Duqu, Gauss, Mahdi, Flame, Wiper, and Shamoon have in common?", CNet, 31 de agosto [www.cnet.com/news/a-whos-who-of-mideast-targeted-malware].

Moore, J. (2015): “Junaid Hussain: How A Boy From Birmingham Became Isis’s Leading Hacker”, Newsweek, 27 de agosto [http://europe.newsweek.com/junaid-hussain-how-boy-birmingham-became-isiss-leading-hacker-332108].

Moreno, D. (2014): “Watch Dogs. Análisis Multiplataforma”, eldiario.es, 5 de junio [www.eldiario.es/juegoreviews/analisis/Watch-Dogs-Analisis-Multiplataforma_0_267723505.html].

Morgan, J. (2014): “A simple explanation od the internet of things”, Forbes, 13 de mayo [www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet- things-that-anyone-can-understand/#227 325086828].

Murphy, L. (2015): “The Curious Case of the Jihadist Who Started Out as a Hacktivist”, Vanity Fair, 15 de diciembre [www.vanityfair.com/news/2015/ 12/isis-hacker-junaid-hussain].

Nakashima, E. (2011): “Cyber-intruder sparks response, debate”, The Washington Post, 8 de diciembre [www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/ 12/06/gIQAxLuFgO_story.html].

Nakashima, E. y Warrick, J. (2012): “Stuxnet was work of U.S. and Israeli experts, officials say”, The Washinton Post, 12 de junio [www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html].

Novack, R. (2015): “We Should Have Seen This Refugee Crisis Coming”, Wired, 22 de septiembre [www.wired.com/2015/09/able-predict-refugee-crisis].

Novetta (2016): “Operation Blockbuster: Unraveling the Long Thread of the Sony Attack”, febrero [www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf].

O’Murchu, L. (2010a): “Distilling the W32.Stuxnet Components”, 22 de julio [www.symantec.com/connect/blogs/distilling-w32stuxnet-components].

— (2010b): “Stuxnet Using Three Additional Zero-Day Vulnerabilities”, Symantec, 14 de septiembre [www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities].

— (2010c): “W32.Stuxnet Installation Details” [www.symantec.com/connect/blogs/w32stuxnet-installation-details].

— (2014); “Countdown to Zero Day-Did Stuxnet escape from Natanz?”, Symantec, 11 de noviembre [www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz].

Padilla, M (2012): El Kit de la lucha en Internet, Traficantes de sueños.

Pagllery, J. (2015): “Se conocen nuevos detalles del hackeo más grande en la historia”; CNN, 6 de agosto [http://cnnespanol.cnn.com/2015/08/06/se-conocen-nuevos-detalles-del-hackeo-mas-grande-en-la-historia/#0].

Peirano, M. (2016a) “Por qué es tan increíble (y preocupante) que una máquina nos gane al Go”, eldiario.es, 12 de marzo [www.eldiario.es/cultura/tecnologia/importante-maquina-pueda-ganar-Go_0_493100959.html].

— (2016b): “Imponer puertas traseras no detendrá el cifrado de datos (ni el terrorismo)”, eldiario.es, 12 de febrero [www.eldiario.es/cultura/tecnologia/privacidad/Imponer-puertas-traseras-detendra-cifrado_0_48365 2441.html].

Perlroth, N. (2012): “Researchers Find Clues in Malware”, The New York Times, 30 de mayo [www.nytimes.com/2012/05/31/technology/resear chers-link-flame-virus-to-stuxnet-and-duqu.html?_r=0].

Pilkington, E. (2015): “Life as a drone operator: ‘Ever step on ants and never give it another thought?’”; The Guardian, 19 de noviembre [www.theguardian.com/world/2015/nov/18/life-as-a-drone-pilot-creech-air-force-base-nevada].

Poulse, K. (2010): “Urban Legend Watch: Cyberwar Attack on U.S. Central Command”, Wired, 31 de marzo [www.wired.com/2010/03/urban-legend].

Quintana, Y. (2014a): “Cómo se comunicaron Snowden y Greenwald para no ser espiados por la NSA”, eldiario.es, 11 de noviembre [www.eldiario.es/turing/vigilancia_y_privacidad/comunicaron-Snowden-Greenwald-espiados-NSA_0_263174096.html].

— (2014b) “Todos los programas de espionaje de la NSA desvelados por Snowden”, eldiario.es, 19 de marzo [www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden _0_2404267 30.html].

— (2014c): “Cómo (y cuánto) puede espiar el gobierno tus llamadas”, eldiario.es, 10 de junio [http://www.eldiario.es/turing/vigilancia_y_privacidad/Vodafone-SITEL-espionaje_telefonico_0_269473073.html].

— (2014d): “Cómo es el ‘Google’ secreto de la NSA y cuáles son sus peligros”, eldiario.es, 4 de septiembre [www.eldiario.es/turing/vigilancia_y_privacidad/Snowden-NSA-ICREACH _0_299220195.html].

— (2014e): “Cómo saltarse un bloqueo de Internet”, eldiario.es, 2 de abril [http://www.eldiario.es/turing/vigilancia_y_privacidad/saltarse-bloqueo-Internet_0_245326216.html].

— (2014f): “La NSA instaló dispositivos de espionaje en equipos informáticos fabricados en Estados Unidos”, eldiario.es, 19 de marzo [http://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-instalando-dispositivos-informaticos-EEUU_0_ 261774670.html].

— (2014g): “Parlamento Europeo: los programas de espionaje masivo vulneran derechos fundamentales y deben prohibirse”, eldiario.es, 11 de marzo [http://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-Parlamento_Europeo-Snowden - espionaje-privacidad_0_237626236.html].

— (2014h): “Pasividad política frente al espionaje masivo de

Estados Unidos", eldiario.es, 8 de mayo [http://www.eldiario.es/turing/vigilancia_y_privacidad/Espionaje-NSA-Snowden-Parlamento_Europeo-Informe_Moraes-Congreso_diputados-ICV-AEPD_0_257924230.html].

— (2015a): "Los sistemas de cifrado que resisten los ataques de la NSA", eldiario.es, 30 de diciembre [www.eldiario.es/turing/criptografia/Nuevas-revelaciones-Snowden-resisten-NSA_0_340515951.html].

Quintana, Y. (coord.) (2015b): "Límites y amenazas al ejercicio de las libertades de expresión e información en España", Plataforma en Defensa de la Libertad de Información.

Quintero Villaroya, J. L. y Estrada Matamala F. (2014): "Ciberguerra: de juegos de guerra a la jungla 4.0", Rooted [http://es.slideshare.net/rootedcon/cosdef-rooted2014-consv3envio].

Reed, B. (ed.) (2015): "Drone Papes", The Intercept, 15 de octubre [https://theintercept.com/drone-papers].

Reuters (2015a): "French broadcaster TV5Monde says it was victim of Islamist hacking"; Bussiness Insider, 9 de abril [www.businessinsider.com/r-french-broadcaster-tv5monde-says-it-was-victim-of-islamist-hacking-2015-4].

— (2015b): "U.S. Drone Strike In Syria Kills Junaid Hussain, Leading Isis Hacker", Newsweek, 27 de agosto [http://europe.newsweek.com/isis-hacker-killed-american-drone-strike-syria-british-junaid-hussain-332101].

Riau, C. (2012): "The Day The Stuxnet Died", Securlist, 25 de junio [https://securelist.com/blog/events/33206/the-day-the-stuxnet-died-27].

Ricker Schulte, S. (2013): Cached. Decoding the Internet in Global Popular Culture, NYPress.

Robertson, J; Riley, M. y Willis, A. (2016): "How to Hack an Election", Bloomberg, 4 de abril.

Ryan, J. (2011): "Tunisia's bitter cyberwar", Al Jazeera, 6 de enero

[www.aljazeera.com/indepth/features/2011/01/20111614145839362.html].

— (2012): “Industrial Control Systems Killed Once and Will Again, Experts Warn”, Wired, 9 de abril [www.wired.com/2008/04/industrial-cont].

Saiz, E. (2013): “La Armada de EE UU hace historia al aterrizar un ‘dron’ en un portaaviones”, El País, 11 de julio [http://internacional.elpais.com/internacional/2013/07/11/actualidad/1373500039_863137.html].

Sánchez, C. (2016): “Un ‘hacker’ español demuestra que los drones de Parrot se pueden secuestrar”, eldiario.es, 4 de marzo [www.eldiario.es/hojaderouter /seguridad/drones-parrot-hacking-seguridad-Bebop_0_491001254.html].

Sandhu, A. (2015): “Snowden criticises Russia for approach to internet and homosexuality”, The Guardian, 5 de septiembre [www.theguardian.com/us-news/2015/sep/05/snowden-criticises-russia-internet-homo sexuality].

Sanger, D. E. (2012): “Obama Order Sped Up Wave of Cyberattacks Against Iran”, The New York Times, 1 de junio [www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0].

Sarabia, D. (2016): “Reino Unido espía a los refugiados hackeando sus móviles y ordenadores”, eldiario.es, 12 de abril.

Scarborough, R. (2015): “Obama plays favorites, protects loose-lipped generals who leak top secret info”, The Washington Times, 12 de marzo [www.washingtontimes.com/news/2015/mar/12/obama-protects-generals-in-leak-probes-while-low-l/?page=all].

Schneier, B. (2005): “Attack Attribution and Cyber Conflict”, Blog Schneier on Security [www.schneier.com/blog/archives/2015/03/attack_attribut_1.html].

— (2013a): “The Battle for Power on the Internet”, Blog Schneier on Security, 30 de octubre [www.schneier.com/blog/

archives/2013/10/the_battle_for_1.html].

— (2013b): “The US government has betrayed the internet. We need to take it back”, The Guardian, 5 de septiembre [www.theguardian.com/com mentisfree/2013/sep/05/gover nment-betrayed-internet-nsa-spying].

Schwarz, J. (2015): “Drones, IBM, And The Big Data Of Death”, The Intercept, 23 de octubre [https://theintercept.com/2015/10/23/ drones-ibm-and-the-big-data-of-death].

Shachtman, N. (2007): “First Armed Robots on Patrol in Iraq”, Wired, 2 de agosto [www.wired.com/2007/08/httpwwwnational].

— (2008): “Under Worm Assault, Military Bans Disks, USB Drives”, Wired, 19 de noviembre [www.wired.com/2008/11/army-bans-usb-d].

— (2009): “Insurgents Intercept Drone Video In King-Size Security Breach — (Updated, With Video)”, Wired, 17 de diciembre [www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach].

— (2010): “Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack — (Updated)”, Wired, 25 de agosto.

— (2011): “Exclusive: Computer Virus Hits U.S. Drone Fleet”, Wired, 7 de octubre [www.wired.com/2011/10/virus-hits-drone-fleet].

Shamah, D. (2012): “Latest viruses could mean ‘end of world as we know it,’ says man who discovered Flame”, The Times of Israel, 6 de junio [www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror].

Shaw, I. G. (2014): “The Rise of the Predator Empire: Tracing the History of U.S. Drones”, Understanding Empire [https:// understandingempire.word press.com/2-0-a-brief-history-of-u-s-drones].

— (2016): “Scorched Atmospheres: The Violent Geographies of the Vietnam War and the Rise of Drone Warfare”, The Annals of the

Association of American Geographers [www.tandfon line.com/doi/full/10.1080/00045608.2015.1115333].

Singer, P. W. y Friedman, A. (2014): Cybersecurity and Cyberwar. What Everyone Needs to Know, Oxford University Press.

SOFREP (2016): “Military ‘Killer’ Robots Closer to Reality? Pentagon Says Yes”, 16 de enero [https://sofrep.com/464 09/killer-robots-drawing-closer-to-a-reality].

Spiegel (2014): “NSA Spied on Chinese Government and Networking Firm”, Spiegel, 22 de marzo [www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960 199.html].

Sputnik News (2016): “Military Prodigy: Russia Develops Advanced Light Tactical Robot”, 13 de enero [http://sputniknews.com/military/2016 0113/1033077331/russia-tactical-robot-military.html#ixzz47zsSx3fi].

Stoyanov, R. (2015): “Russian Financial Cybercrime: How It Works”, Kaspersky, noviembre [https://securelist.com/files/2015/11/Kaspersky_Lab_cybercrime_underground_report_eng_v1_0.pdf].

Symantec (2010a): “W32.Stuxnet: Commonly Asked Questions”, Symanetc, 16 de julio [www.symantec.com/connect /blogs/w32temphid-commonly-asked-questions].

— (2010b): “Dossier sobre Stuxnet”, noviembre de 2010 (actualizado en febrero de 2011) [www.symantec.com /content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf].

— (2013): “Stuxnet 0.5: The Missing Link”, Symanatec, 26 de febrero [www.symantec.com/connect/blogs/stuxnet-05-missing-link].

— (2014): “Los cuatro eventos más destacados de seguridad en Internet del 2014”, [www.symantec.com/con nect/blogs/los-cuatro-eventos-mas-destacados-de-seguridad-en-internet-del-2014].

— (2016): “The Waterbug attack group”, enero [www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf].

Tascón, M. y Quintana, Y. (2012): Ciberactivismo. Las nuevas revoluciones de las multitudes conectadas, Los Libros de la Catarata, Madrid.

Teknautas (2015): “Los asesinatos indiscriminados de EEUU con drones: el 90% son personas inocentes”, El Confidencial, 16 de octubre.

Tenold, V. (2016): “The Untold Casualties of the Drone War”, Rolling Stone, 18 de febrero [www.rollingstone.com/politics / news/the-untold-casualties-of-the-drone-war-20160 218].

Velasco, J. J. (2014): “Las puertas traseras que la NSA nunca reconocerá”, eldiario.es, 15 de agosto [www.eldiario.es/turing/vigilancia_y_privacidad/Vulnerabilidades-puertas-traseras-NSA-reconocera_0_249525793.html].

VirusBlokAda (2010): Ficha sobre ‘Rootkit.TmpHider’ [http://anti-virus.by/en/tempo.shtml].

Weinberger, S. (2010): “What Is SIPRNet?”, Popular Mechanics [www.popularmechanics.com/technology/security/how-to/a6426/what-is-siprnet-and-wikileaks-4085507].

WikiLeaks (2009): “Serious nuclear accident may lay behind Iranian nuke chief’s mystery resignation”, Wikileaks, 17 de julio [https://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief’s_mystery_resig

Yadron, D. (2015): “Iranian Hackers Infiltrated New York Dam in 2013”, The Wall Street Journal, 20 de diciembre [www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559].

Yoste, P. (2013): “Reports: Retired general target of leaks probe”, Associated Press, 28 de junio [http://bigstory.ap.org/article/reports-retired-general-target-leaks-probe].

Zetter, K. (2010a): “Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target”, Wired, 23 de septiembre [www.wired.com/2010/09/stuxnet-2].

— (2010b): “Google Hack Attack Was Ultra Sophisticated, New Details Show”, Wired, 14 de enero [www.wired.com/ 2010/01/ operation-aurora].

— (2010c): “Iran: Computer Malware Sabotaged Uranium Centrifuges”, Wired, 29 de noviembre [www.wired.com/2010/11/ stuxnet-sabotage-centrifuges].

— (2010d): “Report: Critical Infrastructures Under Constant Cyberattack Globally”, Wired, 28 de enero [www.wired.com/2010/01/csis-report-on-cybersecurity].

— (2010e): “SCADA System’s Hard-Coded Password Circulated Online for Years”, Wired, 19 de julio [www.wired.com/2010/07/ siemens-scada].

— (2011a): “H(ackers)2o: Attack On City Water Station Destroys Pum”, Wired, 11 de noviembre [www.wired.com/ 2011/ 11/ hackers-destroy-water-pump].

— (2011b): “Hacker Spies Hit Security Firm RSA”, Wired, 17 de marzo [www.wired.com/2011/03/rsa-hacked].

— (2011c): “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History”, Wired, 11 de julio [www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet].

— (2011d): “The Return of the Worm That Ate the Pentagon”, Wired, 8 de diciembre [www.wired.com/2011/12/worm-pentagon].

— (2012): “Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload”, Wired, 9 de agosto [www.wired.com/2012/08/gauss-espionage-tool].

— (2013a) “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, Wired, 3 de marzo [www.wired.com/2016/03/inside-

cunning -unprecedented-hack-ukraines-power-grid].

— (2013b): “Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon”, Wired, 26 de febrero [www.wired.com/2013/02/new-stuxnet-variant-found].

— (2014a) “Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon”, Crown Publishing/Random House.

— (2014b): “Hacker Lexicon: What Is a Zero Day?”, Wired, 11 de noviembre [www.wired.com/2014/11/what-is-a-zero-day].

— (2014c): “Kaspersky Finds New Nation-State Attack-In Its Own Network”, Wired, 6 de junio [www.wired.com/ 2015/06/ kaspersky-finds-new-nation-state-attack-network].

— (2015a): “The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks”, Wired, 10 de febrero [www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks].

— (2015b): “We’re at Cyberwar: A Global Guide to Nation-State Digital Attacks”, Wired, 1 de septiembre.

— (2016a): “Hacker Lexicon: What Are DoS and DDoS Attacks?”, Wired, 16 de enero [https://www.wired.com/2016 /01/hacker-lexicon-what-are-dos-and-ddos-attacks].

— (2016b): “The Biggest Security Threats We’ll Face in 2016”, Wired, 1 de enero [www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016].

— (2016c): “Why Hospitals Are the Perfect Targets for Ransomware”, Wired, 30 de marzo [www.wired.com/2016/03/ ransomware-why-hospitals-are-the-perfect-targets].

NOTAS

1 . “US redeploys troops to Afghanistan”, Al Jazeera, 10 de septiembre de 2008 [www.aljazeera.com/news/middleeast/2008/09/20089914447155 47.html].

2 . Ficha de Symantec sobre “W32.SillyFDC”, 27 de enero de 2007 [www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99&tabid=2].

3 . Un archivo DLL (Dynamic Library Link) permite ejecutar acciones o rutinas de uso frecuente en diferentes programas de Windows. No son parte de los programas, sino que se guardan como archivos independientes pequeños y así permiten ahorrar espacio en el disco duro y optimizar la memoria RAM.

4 . Recopilación de las encuestas electorales de las elecciones presidenciales de Estados Unidos de 2008: https://en.wikipedia.org/wiki/Nationwide_opinion_polling_for_the_United_States_presidential_election,_200

5 . Declaración de Bush en su visita a la NSA el 24 de octubre de 2008 [http://georgewbush-whitehouse.archives.gov/news/releases/2008/10/20081024-2.html].

6 . “Cracker” frente a “hacker”. Aunque en los medios de comunicación es habitual el uso del término “hacker” como

sinónimo de “pirata informático”, en realidad es incorrecto. “Cracker” es una forma más exacta de referirse a los asaltantes informáticos, mientras que “hacker”, una palabra que denota reconocimiento y prestigio y está vinculada a los orígenes de la informática y de Internet, se refiere a alguien con especial habilidad en los sistemas informáticos. También se aplica a aquellas personas a quien les apasiona saber, descubrir, aprender y, sobre todo, entender el funcionamiento de las cosas. Más información en Tascón y Quintana (2012).

7 . Ficha de Symantec sobre el virus en www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

8 . Ficha de F-Scure sobre Agent.btz en www.f-secure.com/v-descs/worm_w32_agent_btz.shtml

9 . “Agent.btz. A Threat That Hit Pentagon”, 30 de noviembre de 2008 [http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html].

10 . Memorándum del Secretario de Defensa, Robert Gates, ordenando la creación del Mando Cibernético. 23 de junio de 2009 [http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf].

11 . Transcripción completa de la comparecencia disponible en http://fas.org/irp/congress/2010_hr/alexander.html

12 . Citado en Sandhu, 2015.

13 . Consúltese http://jimromenesko.com/2013/04/23/ap-warned-staffers-just-before-ap-was-hacked/

14 . Extracto de una conferencia de Bruce Schneier, uno de los principales expertos del mundo en seguridad informática, sobre el alcance del concepto “ciberguerra” y su uso desproporcionado. Cita íntegra en su blog, “Schneier on Security” [www.schneier.com/blog/archives/2010/10/me_on_cyberwar.html].

15 . Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space (Estado Mayor Conjunto de los Estados Unidos, 2013)

16 . “Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)” [www.nsa.gov/public_info/speeches_testimonies/5may09_dir. shtml].

17 . También puede consultarse The Intercept [https://theintercept.com].

18 . Así ha sido denunciado por instituciones como el Parlamento Europeo, ONG como la Electronic Frontier Fundation (s. f.) y autoridades reconocidas mundialmente como el británico Tim Berne Lee, creador de la web “Tim Berners-Lee: Spies’ cracking of encryption undermines the web”, The Guardian, 3 de diciembre de 2013 [www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden]. Véase también la nota 7.

19 . Five Eyes [https://en.wikipedia.org/wiki/Five_Eyes].

20 . “Sony Pictures Entertainment Hack” [https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack].

21 . Consúltese www.redeszone.net/2016/04/26/los-piratas-informaticos-isis-se-unen-crear-ucc-united-cyber-caliphate/ y www.hackread.com/isis-hackers-united-cyber-caliphate

22 . Consúltese http://europe.newsweek.com/newsweek-twitter-account-hacked-isis-affiliated-group-305897?rm=eu

23 . “IRC (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior. Las conversaciones se desarrollan en los llamados canales de IRC, designados por nombres que habitualmente comienzan con el carácter # o & (este último solo es utilizado en canales locales del servidor) (extraído de Wikipedia).

24 . Texto original completo disponible en archive.org [https://web.archive.org/web/19990910020706/http://www.hackernews.com/archive.html?122998.html].

25 . Puede consultarse www.fbi.gov/news/pressrel/press-releases/

update-on-sony-investigation

26 . Véase https://securelist.com/blog/incidents/65106/south-korean-whois-team-attacks/

27 . Los participantes en la Operación Blockbuster pueden consultarse en https://operationblockbuster.com/participants/index.html

28 . Consúltese https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

29 . https://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/

30 . http://hackstory.net/Hacktivismo

31 . Ibídem.

32 . Fuente: BBC.

33 . Fuente: https://blog.kaspersky.es/

34 . Zetter (2013a) explica los pormenores del ataque, su sofisticada planificación y cómo fue posible hacer caer la red eléctrica

ucraniana, a pesar de su diseño seguro (compartimentada, etc.). Que no fuera preciso un doble factor de autenticación para acceder a su sistema SCADA fue una de las claves. (un doble factor de autenticación es una medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder a un servicio).

35 . Corte de distrito de Estados Unidos. Distrito Sur de Nueva York. Acusación sellada contra: Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan “Nitr0j En26”, Omid Ghaffarinia “Plus”, Sina Keissar y Nader Saedi “Turk Server” [www.justice.gov/opa/file/834996/download].

36 . Puede consultarse http://www.ticbeat.com/seguridad/como-evitar-ataque-ddos/

37 . “Cry havoc! And let slip the maths of war”, The Economist, 31 de marzo de 2011 [www.economist.com/node/18483411].

38 . Fuentes: INCIBE, CNN-CNI, OTAN, CSIS, Symantec, Kaspersky, entre otras.

39 . Para obtener una información más pormenorizada sobre estos datos, el lector puede acudir a (CCDCOE/OTAN, 2016).

40 . Ibídem.

41 . Ibídem.

42 . Ibídem.

43 . Ibídem.

44 . Ibídem.

45 . Ibídem.

46 . Ibídem.

47 . Ibídem.

48 . El retrato de Sergey Ulasen y su intervención en el caso están basados en la entrevista realizada por Eugene Kaspersky (2011).

49 . “Pantalla azul de la muerte” [https://es.wikipedia.org/wiki/Pantalla_azul_de_la_muerte].

50 . Fuentes: Wikipedia y Microsoft Malware Protection Center [https://es.wikipedia.org/wiki/Rootkit] [www.microsoft.com/security/portal/mmpc/threat/rootkits.aspx].

51 . El post completo de Sergey Ulasen, publicado el 12 de julio de 2010, está disponible en www.wilderssecurity.com/threads/rootkit-tmphider.276994

52 . Disponible en www.wilderssecurity.com/threads/rootkit-tmphider.2769 94/#post-1712134

53 . Langner (2013), Wikipedia y adrformacion.com

54 . Ficha de VirusBlokAda sobre Stuxnet "Rootkit.TmpHider" [http://anti-virus.by/en/tempo.shtml].

55 . Ficha de Kaspersky sobre Stuxnet: "Rootkit.Win32.Stuxnet.a", 12 de julio de 2010 [https://w.securelist.com/en/descriptions/rootkit.win32.stuxnet.a]. Ficha de Symantec sobre Stuxnet: "W32.Stuxnet" (13 de julio de 2010) [www.symantec.com/security_response/writeup.jsp?docid=2010-0714 00-3123-99].

56 . Ficha de Micrsoft sobre Stuxnet: "Worm: Win32/Stuxnet.B", Microsoft, 19 de julio de 2010. [www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm%3AWin32%2FStuxnet].

57 . Consúltese www.darpa.mil/program/our-research/darpa-and-the-brain-initiative

58 . Véase www.darpa.mil/program/our-research/darpa-and-the-brain-initiative

59 . “Los drones autónomos ultraveloces se abren paso entre obstáculos”, El País, 17 de febrero de 2016 [http://tecnologia.elpais.com/tecnologia/2016/02/16/actualidad/1455641243_496449.html].

60 Consúltese http://articles.latimes.com/2012/jan/26/business/la-fi-auto-drone-20120126

61 . https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/

62 . Véase www.wired.com/2011/10/virus-hits-drone-fleet/

63 . Véase www.newyorker.com/magazine/2014/11/24/unblinking-stare

64 . Puede consultarse www.aljazeera.com/programmes/specialseries/2016/ 03/drone-cia-secret-drone-war-160330081229214.html

65 . Consúltese http://opencatalog.darpa.mil/DCAPS.html

66 . Las funciones que realizan las máquinas en el ámbito la inteligencia artificial se basan en el reconocimiento de patrones, agrupamiento (clustering), predicción de sucesos y optimización.

67 . “España inaugura su Centro Tecnológico de Seguridad”, informacionsensible.com, 22 de abril de 2016 [www.informacionsensible.com/news/8846/Espana-inaugura-su-Centro-Tecnologico-de-Seguridad].

68 . Fuentes: Quintana (2014b; 2014d; 2014f) y Gonzalo y Quintana (2014).

69 . Fuente: Quintana (2014c).

70 . Fuente: Quintana (2014e).

71 . http://www.wired.com/2016/03/truth-and-power/

72 . Fuentes: Kelh, Wilson y Banskton (2015); Geller (2016).

73 . Fuente: http://hackstory.net/Kript%C3%B3polis.